09/404,547

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ９月３０日

出 願 番 号
Application Number: 平成１０年特許願第２９２８２４号

出 願 人
Applicant (s): 株式会社東芝

１９９９年 ４月１６日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

【書類名】　特許願
【整理番号】　A009806136
【提出日】　平成10年 9月30日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/00
【発明の名称】　中継装置及び通信装置
【請求項の数】　21
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　斉藤　健
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　高畠　由彰
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【書類名】　明細書

【発明の名称】　中継装置及び通信装置

【特許請求の範囲】

【請求項１】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信する代理構成手段と、

前記第１のネットワーク上の装置からの前記第１の情報を受信した際、この情報が少なくとも所定の情報であるか否かを検出する検出手段と、

前記検出手段により、検出した第１の情報が前記所定の情報であった場合には、前記所定の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニットに転送する転送手段とを具備したことを特徴とする中継装置。

【請求項２】

前記所定の情報は、前記第１のネットワーク上の装置と前記第２のネットワーク上の装置またはサービスまたはサブユニット間で送受信される情報を保護するための情報であり、少なくとも認証手続きに関する情報からなることを特徴とする請求項１に記載の中継装置。

【請求項３】

前記第１のインタフェース手段または前記第２のインタフェース手段から特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段または前記第２のインタフェース手段の一方から受信された前記特定のコンテンツを含むデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備したことを特徴とする請求項２に記載の中継装置。

【請求項４】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信する代理構成手段と、

前記第１のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、

前記第２のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続き行う第２のコピープロテクション処理手段とを具備し、

前記代理構成手段は、前記第１のネットワーク上の装置と前記第２のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１のコピープロテクション処理手段を用いて該第１のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第２のコピープロテクション処理手段を用いて前記第２のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする中継装置。

【請求項５】

前記第２のコピープロテクション処理手段による前記所定のコンテンツ保護手続の相手は、前記代理構成手段が代理サービスを提供している前記第２のネットワーク上の装置またはサービスまたはサブユニットであることを特徴とする請求項４に記載の中継装置。

【請求項６】

前記第１のインタフェース手段または前記第２のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段または前記第２のインタフェース手段の一方か

ら受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備したことを特徴とする請求項４に記載の中継装置。

【請求項７】

少なくとも前記復号化手段および前記暗号化手段は同一のＬＳＩに封止されていることを特徴とする請求項６に記載の中継装置。

【請求項８】

前記特定のコンテンツは前記所定のコンテンツ保護手続きにて保護されるコンテンツであることを特徴とする請求項３または６に記載の中継装置。

【請求項９】

前記第２のネットワーク上の装置またはサービスまたはサブユニットを構成認識する構成認識手段をさらに具備したことを特徴とする請求項２または４に記載の中継装置。

【請求項１０】

前記代理構成手段は、さらに、前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第３の情報を、代理で受信し、前記第１のネットワーク上の装置またはサービスまたはサブユニットへの第４の情報に変換して、送信することを特徴とする請求項２または４に記載の中継装置。

【請求項１１】

前記代理構成手段は、前記第１のネットワークの装置に対してデータを送信する際に、あらかじめ該第１のネットワークの装置に対して自中継装置が代理構成

している該データを送信する装置またはサービスまたはサブユニットを通知することを特徴とする請求項２または４に記載の中継装置。

【請求項１２】

第１のネットワークに接続された第１のインタフェース手段と、

前記第１のネットワークに接続された所定の中継装置を介して通信可能な第２のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続を含む所定のコンテンツ保護手続きを行うコピープロテクション処理手段とを具備したことを特徴とする通信装置。

【請求項１３】

前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、

このパケット送受信手段は、前記中継装置が、前記第２のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この代行サービスを通して該第２のネットワーク上の装置またはサービスまたはサブユニットとの間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うことを特徴とする請求項１２に記載の通信装置。

【請求項１４】

前記コピープロテクション処理手段は、前記第２のネットワーク上の装置またはサービスまたはサブユニットの持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つことを特徴とする請求項１３に記載の通信装置。

【請求項１５】

前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、

このパケット送受信手段は、前記中継装置が、前記第２のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この中継装置との間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うことを特徴とする請求項１２に記載の通信装置。

【請求項１６】

前記コピープロテクション処理手段は、前記中継装置の持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つことを特徴とする請求項１５に記載の通信装置。

【請求項１７】

前記中継装置に対して、前記コピープロテクション処理手段が認証フォーマットを持つことを示す情報を含む自通信装置の構成情報を送信する送信手段をさらに具備したことを特徴とする請求項１２に記載の通信装置。

【請求項１８】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第１のコピープロテクション処理手段と、

第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第２のコピープロテクション処理手段と、

前記第１のインタフェース手段または前記第２のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段または前記第２のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項１９】

前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信するとともに、前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第３の情報を、代理で受信し、前記第１のネットワーク上の装置またはサービスまたはサブユニットへの第４の情報に変換して、送信する代理構成手段をさらに具備し、

前記代理構成手段は、前記第１および第２のネットワークの一方のネットワーク上の装置と前記第１および第２のネットワークの他方のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方を用いて該一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記他方のネットワーク上の装置またはサービスまたはサブユニットと、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方を用いて、該所定のコンテンツ保護手続きを行うことを特徴とする請求項１８に記載の中継装置。

【請求項２０】

前記コンテンツ受信手段は、前記第２のコピープロテクション処理手段を用いて、前記第２のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第１のコピープロテクション処理手段を用いて、前記第１のネットワークの装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うことを特徴とする請求項１８に記載の中継装置。

【請求項２１】

第１の装置の制御に供される画面描画のためのプログラムを含む、第１の制御プログラムを受信し、これを稼働するプロセッサ手段と、

このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、

前記パネル画面へのコマンドと、前記第１の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、

前記パネル画面をサブユニットとして第２の装置に公開するサブユニット処理手段と、

前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第１の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＥＥＥ１３９４バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及び無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【０００２】

【従来の技術】

近年、デジタル放送の開始や、デジタルＡＶ機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】

しかしながら、このデジタルＡＶ技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どおりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」

の問題が発生する。

【０００４】

この「不正コピー」を防ぐための技術がいくつか検討されている。その中の一つが、ＣＰＴＷＧ（コピープロテクション技術ワーキンググループ）で検討されている「１３９４ＣＰコンテンツ保護システム仕様（１３９４ＣＰ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ Ｓｐｅｃｉｆｉｃａｔｉｏｎ）」である。この技術は、ＩＥＥＥ１３９４バスに接続されたノード間で、転送するコンテンツ（例えばＭＰＥＧデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【０００５】

【発明が解決しようとする課題】

ＩＥＥＥ１３９４バスは、最低速度でも１００Ｍｂｐｓ、網そのものに自動構成認識機能が備わっている、ＱＯＳ転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルＡＶ向けのネットワークとして、デファクトスタンダードの地位を築いている。

【０００６】

しかし、ＩＥＥＥ１３９４は、これら特徴のゆえに、「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とＩＥＥＥ１３９４バスを接続する場合は、これらの網が１００Ｍｂｐｓ以上といった高速性を一般には有していないことや、ＩＥＥＥ１３９４の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれな

いことから、ＩＥＥＥ１３９４プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、ＩＥＥＥ１３９４と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等が提案されている。

【０００７】

これらの方法を、従来の技術で述べた１３９４コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術がＩＥＥＥ１３９４バスについてのみ定められている状況である。このコピープロテクション技術を「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【０００８】

本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をＩＥＥＥ１３９４のみならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【０００９】

また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明（請求項１）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信する代理構成手段と、前記第１のネットワーク上の装置からの前記第１の情報を受信した際、この情報が少なくとも所定の情報であるか否かを検出する検出手段と、前記検出手段により、検出した第１の情報が前記所定の情報で

あった場合には、前記所定の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニットに転送する転送手段とを具備したことを特徴とする。

【００１１】

好ましくは、本発明（請求項２）のように、請求項１に記載の中継装置において、前記所定の情報は、前記第１のネットワーク上の装置と前記第２のネットワーク上の装置またはサービスまたはサブユニット間で送受信される情報を保護するための情報であり、少なくとも認証手続きに関する情報からなるものであるようにしてもよい。

【００１２】

本発明（請求項２）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第２のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニットを装置等と呼ぶ）」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えることなく中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において行うことができる。

【００１３】

なお、少なくとも認証手続きを含むコンテンツ保護手続きは、例えば、認証手続き、認証手続きおよび鍵交換手続き、などである。

【００１４】

好ましくは、本発明（請求項３）のように、請求項２に記載の中継装置において、前記第１のインタフェース手段または前記第２のインタフェース手段から特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のイン

タフェース手段または前記第２のインタフェース手段の一方から受信された前記特定のコンテンツを含むデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備するようにしてもよい。

【００１５】

本発明（請求項３）によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、請求項２にて処理されるコンテンツ保護形式にて、そのコンテンツを保護された形でエンドエンドに送り届けることができる。

【００１６】

本発明（請求項４）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信する代理構成手段と、前記第１のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、前記第２のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続き行う第２のコピープロテクション処理手段とを具備し、前記代理構成手段は、前記第１のネットワーク上の装置と前記第２のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１のコピープロテクション処理手段を用いて該第１のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第２のコピープロテクション処理手段を用いて前記第２のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする。

【００１７】

本発明（請求項４）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第２のネットワーク上の装置等」と中継装置との間、および中継装置と「第１のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００１８】

好ましくは、本発明（請求項５）のように、請求項４に記載の中継装置において、前記第２のコピープロテクション処理手段による前記所定のコンテンツ保護手続の相手は、前記代理構成手段が代理サービスを提供している前記第２のネットワーク上の装置またはサービスまたはサブユニットであるようにしてもよい。

本発明（請求項５）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「代理構成手段が提供している第２のネットワーク上の装置等」と中継装置との間、および中継装置と「第１のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００１９】

好ましくは、本発明（請求項６）のように、請求項４に記載の中継装置において、前記第１のインタフェース手段または前記第２のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のインタフェース手段または前記第２のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備するようにしてもよい。

【００２０】

本発明（請求項６）によれば、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【００２１】

好ましくは、本発明（請求項７）のように、請求項６に記載の中継装置において、少なくとも前記復号化手段および前記暗号化手段は同一のＬＳＩに封止されているようにしてもよい。

【００２２】

本発明（請求項７）によれば、この復号化手段と暗号化手段との間は、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【００２３】

好ましくは、本発明（請求項８）のように、請求項３または６に記載の中継装置において、前記特定のコンテンツは前記所定のコンテンツ保護手続きにて保護

されるコンテンツであるようにしてもよい。

【００２４】

本発明（請求項８）によれば、保護されるべきコンテンツをエンドエンドに転送することができる。

【００２５】

好ましくは、本発明（請求項９）のように、請求項２または４に記載の中継装置において、前記第２のネットワーク上の装置またはサービスまたはサブユニットを構成認識する構成認識手段をさらに具備するようにしてもよい。

【００２６】

本発明（請求項９）によれば、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【００２７】

好ましくは、本発明（請求項１０）のように、請求項２または４に記載の中継装置において、前記代理構成手段は、さらに、前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第３の情報を、代理で受信し、前記第１のネットワーク上の装置またはサービスまたはサブユニットへの第４の情報に変換して、送信するようにしてもよい。

【００２８】

本発明（請求項１０）によれば、コンテンツ保護手続きとして、第２のネットワーク上の装置等から、第１のネットワーク上の装置等への方向の手続きが必要な場合に、当該中継装置がその仲立ちを行うことができる。

【００２９】

好ましくは、本発明（請求項１１）のように、請求項２または４に記載の中継装置において、前記代理構成手段は、前記第１のネットワークの装置に対してデータを送信する際に、あらかじめ該第１のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。

【００３０】

本発明（請求項１１）によれば、この通知を受信した第１のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【００３１】

本発明（請求項１２）に係る通信装置は、第１のネットワークに接続された第１のインタフェース手段と、前記第１のネットワークに接続された所定の中継装置を介して通信可能な第２のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続を含む所定のコンテンツ保護手続きを行うコピープロテクション処理手段とを具備したことを特徴とする。

【００３２】

本発明（請求項１２）によれば、直接第１のネットワークで接続されていない装置等との間で、コンテンツ保護手続きを行うことができるようになる。

【００３３】

好ましくは、本発明（請求項１３）のように、請求項１２に記載の通信装置において、前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、このパケット送受信手段は、前記中継装置が、前記第２のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この代行サービスを通して該第２のネットワーク上の装置またはサービスまたはサブユニットとの間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うようにしてもよい。

本発明（請求項１３）によれば、第２のネットワーク上の装置等と直接の通信機能を持っていない場合においても、パケットの送受信先を中継装置の代理サービスとし、この代理サービスを通して、第２のネットワーク上の装置等と、コンテンツ保護手続きを行うことができるようになる。

【００３４】

好ましくは、本発明（請求項１４）のように、請求項１３に記載の通信装置において、前記コピープロテクション処理手段は、前記第２のネットワーク上の装置またはサービスまたはサブユニットの持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つようにしてもよい。

【００３５】

本発明（請求項１４）によれば、同一の認証機関が定めたコンテンツ保護手続きを、自通信装置と第２のネットワーク上の装置等とのエンドエンド間で行うことができる。

【００３６】

好ましくは、本発明（請求項１５）のように、請求項１２に記載の通信装置において、前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、このパケット送受信手段は、前記中継装置が、前記第２のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この中継装置との間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うようにしてもよい。

本発明（請求項１５）によれば、第２のネットワーク上の装置等との直接の通信機能を持っていない場合においても、パケットの送受信先を中継装置の代理サービスとし、自通信装置と中継装置との間でコンテンツ保護手続きを行い、第２のネットワーク上の装置等と中継装置との間のコンテンツ保護手続きについては、中継装置にまかせることで、結局、エンドエンドのコンテンツ保護手続きを行うことができる。

【００３７】

好ましくは、本発明（請求項１６）のように、請求項１５に記載の通信装置において、前記コピープロテクション処理手段は、前記中継装置の持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つようにしてもよい。

【００３８】

本発明（請求項１６）によれば、同一の認証機関が定めたコンテンツ保護手続きを、自通信装置と中継装置とのエンドエンド間で行うことができる。

【００３９】

好ましくは、本発明（請求項１７）のように、請求項１２に記載の通信装置において、前記中継装置に対して、前記コピープロテクション処理手段が認証フォーマットを持つことを示す情報を含む自通信装置の構成情報を送信する送信手段

をさらに具備するようにしてもよい。

【００４０】

本発明（請求項１７）によれば、中継装置に対して、自通信装置に暗号化データを送信することが可能であることを通知することができる。また、中継装置がこの通知を第２のネットワーク上に開示等することで、第２のネットワーク上の装置は、その旨を知ることができる。

【００４１】

本発明（請求項１８）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第１のコピープロテクション処理手段と、第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第２のコピープロテクション処理手段と、前記第１のインタフェース手段または前記第２のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のインタフェース手段または前記第２のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第１のインタフェース手段または前記第２のインタフェース手段の他方へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【００４２】

本発明（請求項１８）によれば、第１のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第１のネットワークと第２のネットワークの通信帯域が著しく異なる場合のように、第２のネットワークに元のデータと

は異なるデータ形式で転送することが求められた場合に、変換手段によってデータ形式の変換を行いつつ、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【００４３】

好ましくは、本発明（請求項１９）のように、請求項１８に記載の中継装置において、前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第１の情報を、代理で受信し、前記第２のネットワーク上の装置またはサービスまたはサブユニットへの第２の情報に変換して、送信するとともに、前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第３の情報を、代理で受信し、前記第１のネットワーク上の装置またはサービスまたはサブユニットへの第４の情報に変換して、送信する代理構成手段をさらに具備し、前記代理構成手段は、前記第１および第２のネットワークの一方のネットワーク上の装置と前記第１および第２のネットワークの他方のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する一方を用いて該一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記他方のネットワーク上の装置またはサービスまたはサブユニットと、前記第１のコピープロテクション処理手段または前記第２のコピープロテクション処理手段の該当する他方を用いて、該所定のコンテンツ保護手続きを行うようにしてもよい。

【００４４】

本発明（請求項１９）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方の

ネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間で、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００４５】

好ましくは、本発明（請求項２０）のように、請求項１８に記載の中継装置において、前記コンテンツ受信手段は、前記第２のコピープロテクション処理手段を用いて、前記第２のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第１のコピープロテクション処理手段を用いて、前記第１のネットワークの装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。

本発明（請求項２０）によれば、第２のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第２のネットワーク上の装置等と認証手続きを行い、その後、第１のネットワーク上の装置等との認証に失敗した場合に、第１のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

【００４６】

本発明（請求項２１）に係る通信装置は、第１の装置の制御に供される画面描画のためのプログラムを含む、第１の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第１の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と

、前記パネル画面をサブユニットとして第２の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第１の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。

【００４７】

一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよいため、簡単な計算環境を用意しておけばよい。本発明（請求項２１）によれば、前記制御プログラムを持たない第２の装置に対しても、パネル画面という形で、前記第１の装置の制御インタフェースを提供することが可能になる。

【００４８】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００４９】

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００５０】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００５１】

（第１の実施形態）

図１は、ある家庭のホームネットワークの全体構成の一例である。

【００５２】

このホームネットワークには、送信ノード１０１、中継ノード１０２、無線ノード１０３の３つが接続されており、送信ノード１０１と中継ノード１０２は（

有線の）ＩＥＥＥ１３９４バス１０４に、中継ノード１０２と無線ノード１０３は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

【００５３】

本実施形態では、送信ノード１０１から送出されたＭＰＥＧ映像を、中継ノード１０２で中継し、無線区間を経由して無線ノード１０３に送信する場合を例として説明する。その際に、著作権保護（不正コピーの防止）のために、送信ノード１０１と無線ノード１０３との間で転送されるＭＰＥＧ映像データは暗号化される場合を考える。

【００５４】

なお、図１では、３つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい（後述する他の実施形態においても同様である）。

【００５５】

図２に、送信ノード１０１の内部構造の一例を示す。

【００５６】

送信ノード１０１は、内部にＭＰＥＧ映像データを蓄積している装置であり、要求に応じてＭＰＥＧ映像データをＩＥＥＥ１３９４バス１０４を通じて送出する。その際、ＩＥＥＥ１３９４バス上において不法コピーをされることを未然に防止するために、必要な場合には送出するＭＰＥＧ映像データを暗号化して送出する機能を持つ。そのため、ＭＰＥＧ映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

【００５７】

図２に示されるように、この送信ノード１０１は、ＩＥＥＥ１３９４インタフェース４０１、ＡＶ／Ｃプロトコルの処理を行うＡＶ／Ｃプロトコル処理部４０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部４０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち、同期チャネルを通してやり取りされるデータについて送受信するＩＳＯ信号送受信部４０４、ＭＰＥＧ映像のストレージであるＭＰＥＧストレージ部４０６、コピープロテクション処理部４０３から暗号鍵Ｋをもらい、ＭＰＥＧ映像を暗

号化してＩＳＯ信号送受信部４０４に送出する暗号化部４０５を有する。ここで、コピープロテクション処理部４０３は、認証のためのフォーマットＡｃｅｒｔを持つ。

【００５８】

次に、図３に、中継ノード１０２の内部構造の一例を示す。

【００５９】

中継ノード１０２は、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能の他に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能が存在する。

【００６０】

図３に示されるように、この中継ノード１０２は、ＩＥＥＥ１３９４インタフェース２０１、無線インタフェース２０２、ＡＶ／Ｃプロトコル処理部２０３、ＩＳＯ信号送受信部２０４、無線区間側の同期チャネルの信号の送受信を行う無線ＩＳＯ信号送受信部２０５、ＩＥＥＥ１３９４バス上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）をＩＥＥＥ１３９４上に広告する機能を持つ１３９４バス構成認識部２０６、ＩＥＥＥ１３９４バス側に対して無線区間側のノードやサービス（サブユニット）を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してＩＥＥＥ１３９４側のノード／サービス（サブユニット）の代理公開やコマンドの代理受付／翻訳等を行う代理サブユニット構成部２０７、無線区間上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）を無線区間上に広告する機能を持つ無線区間構成認識部２０９、コピープロテクションに関する処理を行い、１３９４バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御／フ

ォワード部２１０、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部２１１を有する。

【００６１】

次に、図４に、無線ノード１０３の内部構造の一例を示す。

【００６２】

無線区間においていわゆるＩＥＥＥ１３９４プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、ＩＥＥＥ８０２．１１や無線ＬＡＮ等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆるＱＯＳ機能（同期通信機能）を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分にＱＯＳ機能が求められると制限されるものではない。

【００６３】

いわゆるＩＥＥＥ１３９４ノードではない無線ノード１０３が、ＩＥＥＥ１３９４バスにつながれたノード（本実施形態では送信ノード１０１）と通信を行うために、前述のように、中継ノード１０２がＩＥＥＥ１３９４バス上のノードや機能（サブユニット）をエミュレートしている。すなわち、無線ノード１０３から見て、中継ノード１０２はいわゆるＩＥＥＥ１３９４バス側のノードや機能の代理サーバとなっている。無線ノード１０３は、これら（ＩＥＥＥ１３９４側のノードや機能）を中継ノード１０２の機能と考え、通信を行うが、実際には中継ノード１０２が必要なプロトコル変換やデータの乗せ換えを行う。

【００６４】

図４に示されるように、この無線ノード１０３は、無線インタフェース３０１、無線ノード制御パケット送受信部３０２、コピープロテクション処理部３０３、無線ＩＳＯ信号送受信部３０４、受信した暗号化されたストリーム（ＭＰＥＧ映像等）を、コピープロテクション処理部３０３から渡されるコンテンツキーＫを使ってこれを復号化する暗号復号化部３０５、ＭＰＥＧデコード部３０６、映像を表示するディスプレイ部３０７を有する。

【００６５】

無線ノード１０３のコピープロテクション処理部３０３は、後述するように、

認証フォーマットＢｃｅｒｔを持ち、その認証の発行機関は、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔの発行機関と同一の発行機関である。

【００６６】

次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図５／図６（全体のシーケンス例）、図７／図８（送信ノード１０１のフローチャート例）、図９／図１０／図１１（中継ノード１０２のフローチャート例）、図１２／図１３（無線ノード１０３のフローチャート例）を参照しながら説明する。

【００６７】

まず、無線ノード１０３は、自分の構成情報を中継ノード１０２に通知する（ステップＳ５０１）。この通知は、無線ノード内にＩＥＥＥ１２１２レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、ＩＥＥＥ１３９４向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

【００６８】

ここで、認証について簡単に説明する。

【００６９】

ネットワーク上を映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能となってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

【００７０】

次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たとえ、データを暗号化して送ったとしても、送った先のノード

（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

【００７１】

具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上を転送する、という手法をとる。

【００７２】

さて、無線ノード１０３は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード１０３が持っている認証フォーマットを「Ｂｃｅｒｔ」とする。

【００７３】

無線ノード１０３は、図５のステップＳ５０１で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップＳ８０１）。例えば、図１４のように、構成情報の中に、本無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

【００７４】

なお、中継ノード１０２が無線ノード１０３の構成を認識する方法としては、この他にも中継ノード１０２が無線ノード１０３に対して構成を問い合わせるパケットを送信し、無線ノード１０３がこれに答える方法等も可能である。

【００７５】

さて、この構成情報を受信した中継ノード１０２は、無線ノード１０３が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ７０１）。

【００７６】

中継ノード１０２は、無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継ノード１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ５０２）。具体的には、ＩＥＥＥ１２１２レジスタに「自分はＭＰＥＧデコード／ディスプレイ機能を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、ＩＥＥＥ１３９４に接続されたノードは、中継ノード１０２にこの機能が存在すると認識することになる）。

【００７７】

そのために、中継ノード１０２は、代理サブユニット構成部２０７内に代理テーブル２０８を持つ。代理テーブル２０８は、図１５／図１６のように、中継ノード１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【００７８】

ここでは、図１５のように、無線ノード１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ７０２，Ｓ７０３）。

【００７９】

このため、送信ノード１０１から見た中継ノード１０２の構造は図１７のよう

に見えることになる（ステップＳ６０１）。

【００８０】

以上は、ＩＥＥＥ１３９４バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図１６のような設定がなされ、無線ノードから見た中継ノード１０２の構造は図１８のように見える。

【００８１】

さて、中継ノード１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャネル＃ｘを確立し、ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ）と、ＭＰＥＧデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令をだす（ステップＳ５０３，Ｓ６０２）。送信ノード１０１は、このサブユニットが中継ノード１０１にあたるものと解釈しているため、命令の送信先は中継ノード１０２である。

【００８２】

これを受信（ステップＳ７０４）した中継ノード１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２０８を参照して、この命令先の実体は無線ノード１０３にあることを認識する（ステップＳ７０５）。

【００８３】

よって、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャネル（＃ｙ）の確保を行い（ステップＳ７０６）、さらにＩＳＯ信号送受信部２０４（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２０５（同期チャネル＃ｙを送信）を接続し、１３９４インタフェース２０１から入力された入力データ（ＩＳＯデータ）を無線区間にフォワードできるようにする（ステップＳ５０４，Ｓ７０７）。

【００８４】

さらに、無線ノード１０３に対して、「無線同期チャネル＃ｙを通してデータを送信するので、これを受信し、ＭＰＥＧデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する（ステップＳ５０５，Ｓ７０８）。

【００８５】

図１９に、この無線ノード制御パケットの一例を示す。

【００８６】

図１９に示されるように、無線ノード１０３に無線同期チャネル＃ｙを通して送信したデータ（ＭＰＥＧ映像）を、ＭＰＥＧデコード／ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ（ＭＰＥＧ映像）を送信するサブユニット（中継ノード１０２の映像送信機能；実際には、送信ノード１０１の代理でその機能を持っていると広告している）についての情報も併せて通知している。

【００８７】

これを受信した無線ノード１０３は、無線同期チャネル＃ｙを通してデータが送られてくることを認識する（ステップＳ８０２）。無線ノード１０３は、このデータの送信元は中継ノード１０２の映像送信サブユニットであると認識する（前述のように、実際のデータ送信元は送信ノード１０１である）。このため、この無線ノード制御パケット内に、「この無線同期チャネルを通して送信されるデータの送信元は中継ノード１０２の映像送信サブユニットである」との情報を含めてもよい。

【００８８】

この後、送信ノード１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ６０３，Ｓ５０６）。これを受信した中継ノード１０２は、先に設定したようにこれを無線区間にフォワードする（ステップＳ７０９，Ｓ５０７）。

【００８９】

このようにして、暗号化されたＭＰＥＧ映像が無線ノード１０３に到達する（

ステップＳ８０３）。しかし、この時点で無線ノード１０３はこの暗号を解くための鍵を有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、ここから暗号を解いて、ＭＰＥＧ映像を取り出すことはできない。ここで、無線ノード１０３は認証手続きがＭＰＥＧ映像の送信元と必要であることを認識する。

【００９０】

そこで、無線ノード１０３（のコピープロテクション処理部３０３）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード１０３には、上記暗号化データの送信元は中継ノード１０２（内の映像送信サブユニット）であるように認識されているので、認証要求の宛先も、中継ノード１０２（内の映像送信サブユニット）である。その際、認証要求には、無線ノード１０３の認証フォーマットＢｃｅｒｔ等を付与する（ステップＳ８０４，Ｓ５０８）。

【００９１】

これを受信（ステップＳ７１０）した中継ノード１０２は、代理テーブル２０８を参照して、この認証要求の要求先が実は送信ノード１０１（の映像送信サブユニット）であることを認識し、この認証要求を、中身を変えずに（Ｂｃｅｒｔ等はそのまま残して）送信ノード１０１に対してフォワードする（ステップＳ５０９，Ｓ７１１）。

【００９２】

ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード１０１に到達することになり、結局送信ノード１０１と無線ノード１０３との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード１０２をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【００９３】

これを受け取った送信ノード１０１は、これを中継ノード１０２のＭＰＥＧデコード／ディスプレイサブユニットから送られてきた認証要求であると解釈する

（ステップＳ６０４）。その後、Ｂｃｅｒｔから無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットを特定できるＩＤ（Ｂｄｉｄ）を抽出し（ステップＳ６０５）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード１０１は、Ｂｃｅｒｔが無線ノード１０３の認証フォーマットであるとは意識することはなく、むしろ中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマットであると意識をしている。

【００９４】

この認証要求には、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔと、Ｂｄｉｄとが含まれる。ここで、送信ノード１０１は、該認証要求Ｓ５０９の送信元は中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる（ステップＳ６０６，Ｓ５１０）。

【００９５】

これを受信（ステップＳ７１２）した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続の本来の要求先が無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）であることを認識し、この認証手続要求を、中身を変えずに（Ａｃｅｒｔ等はそのまま残して）無線ノード１０３に対してフォワードする（ステップＳ５１１，Ｓ７１３）。この認証要求の送信元は中継ノード１０２である。

【００９６】

これを受け取った無線ノード１０３は、これを中継ノード１０２の映像送信サブユニットから送られてきた認証要求であると解釈する（ステップＳ８０５）。その後、Ａｃｅｒｔから送信ノード１０１の映像サブユニットを特定できるＩＤ（Ａｄｉｄ）を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード１０３は、Ａｃｅｒｔが送信ノード１０１の認証フォーマットであるとは意識せず、むしろ中継ノード１０２（の映像送信サブユニット）の認証フォーマットであると意識する。

【００９７】

この認証鍵の交換に必要な残りの手続きとして、無線ノード１０３は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップＳ５１２）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、Ａｃｅｒｔの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスＩＤ（Ａｄｉｄ）等が含まれている（ステップＳ８０６）。ここで、無線ノード１０３は、該認証要求Ｓ５１１の送信元は中継ノード１０２（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる。

【００９８】

これを受信した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続きの本来の要求先が送信ノード１０１（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード１０１に対してフォワードする（ステップＳ５１３，Ｓ７１４）。このパケットの送信元は中継ノード１０２である。

【００９９】

これと同様の手続きが送信ノード１０１→中継ノード１０２→無線ノード１０３の方向に対しても行われる（ステップＳ５１４，Ｓ５１５，Ｓ６０９，Ｓ７１５，Ｓ８０７）。

【０１００】

この認証手続きパケットを受信した送信ノード１０１および無線ノード１０３は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Ｋａｕｔｈを導き出す。この共通の認証鍵Ｋａｕｔｈは、送信ノード（の映像送信サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵Ｋａｕｔｈを、この両者（送信ノード１０１、無線ノード１０３）以外の他人に知られることなく共有することがこの時点でできるようになる（ステップＳ６０８，Ｓ８０８）。

【０１０１】

この認証鍵Ｋａｕｔｈを使って、実際にＭＰＥＧストリームの暗号化を行うコンテンツキーＫの計算ができるようになる。

【０１０２】

さて、このようにして、送信ノード１０１（の映像送信サブユニット）と無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）との間で、コンテンツキーＫの値が共有できるようになった。

【０１０３】

ここで、送信ノード１０１が、送信するＭＰＥＧ映像を、コンテンツキーＫを使って、暗号化部４０５にて暗号化し（ステップＳ６１０）、これを１３９４バスの同期チェネル＃ｘを通して中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に対して送信する（ステップＳ５１６，Ｓ６１１）。

【０１０４】

中継ノード１０２は、送信ノード１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部２０４から無線ＩＳＯ信号送受信部２０５を通して、無線同期チャネル＃ｙに送信する（ステップＳ５１７，Ｓ７１６）。

【０１０５】

これを受信した無線ノード１０３は、キーＫの値を使ってＭＰＥＧ映像の値を復号化する（ステップＳ８１０）。復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部３０６にて復号化され、これをディスプレイ部３０７にて再生表示する。

【０１０６】

このように、１３９４バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード１０１と無線ノード１０３）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継ノード１０２を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送も、コピーが不可能なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境に

おいても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０１０７】

なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第２の実施形態で説明するので、例えばこれを適用すればよい。

【０１０８】

また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【０１０９】

（第２の実施形態）

次に、第２の実施形態について説明する。

【０１１０】

第１の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード（の映像サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのＭＰＥＧデコード／ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【０１１１】

これに対し、第２の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノ

ードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、１３９４バス区間のＭＰＥＧデータの暗号化転送についての責任を終端するとともに、無線区間のＭＰＥＧデータの暗号化転送についての責任を終端する場合の例である。

【０１１２】

図２０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１１３】

図２１に、送信ノード２１０１の内部構造の一例を示す。これも第１の実施形態と基本的には同様である。

【０１１４】

次に、図２２に、中継ノード２１０２の内部構造の一例を示す。

【０１１５】

中継ノード２１０２は、第１の実施形態と同様に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。

【０１１６】

また、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能を持つが、第１の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間と無線区間との両方について、この中継ノード２１０２において終端されており、ＩＥＥＥ１３９４バス側については認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部２２０８に、無線区間側については認証フォーマットＣｃｅｒｔを無線区間コピープロテクション処理部２２１２にそれぞれ持ち、１３９４バスの同期チャネルから入力されてきた暗号化データに

ついては、ＩＳＯ信号受信部２２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ映像を、暗号化部２２０５にて再暗号化→無線ＩＳＯ信号送受信部２２０６にて、無線同期信号上に送信、というプロセスを踏む点である。

【０１１７】

ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１１８】

次に、図２３に、無線ノード２１０３の内部構造の一例を示す。コピープロテクション処理部２３０３が、無線区間向けの認証フォーマットＤｃｅｒｔを持っていること以外は、基本的には第１の実施形態の無線ノードと同様である。

【０１１９】

次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図２４／図２５（全体のシーケンス例）、図２６／図２７（送信ノード２１０１のフローチャート例）、図２８／図２９／図３０（中継ノード２１０２のフローチャート例）、図３１／図３２（無線ノード２１０３のフローチャート例）を参照しながら説明する。

【０１２０】

まず、無線ノード２１０３は、自分の構成情報を中継ノード２１０２に通知する（ステップＳ２５０１）。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つことといったことや、認証のための認証フォーマットを持っていることなどである（図１４参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップＳ２８０１）。

【０１２１】

これを受信した中継ノード２１０２は、無線ノード２１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ２７０１）。中継ノード２１０２は、第１の実施形態と同様に、このＭＰＥＧデコード／ディスプレイ機能を、ＩＥＥＥ１２１２レジスタやＡＶ／Ｃプロトコル等を使って、中継ノード２１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ２５０２）。

【０１２２】

そのために、中継ノード２１０２は、代理サブユニット構成部２２１０内に代理テーブル２２１４を持つ。この代理テーブル２２１４は、基本的には第１の実施形態と同様であり、図３３／図３４のように、中継ノード２１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１２３】

ここでは、図３３のように、無線ノード２１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ２７０２，Ｓ２７０３）。

【０１２４】

このため、送信ノード２１０１から見た中継ノード２１０２の構造は、図３５のように見えることになる（ステップＳ２７０２，Ｓ２７０３）。

【０１２５】

以上は、ＩＥＥＥ１３９４バス側についての説明であったが、第１の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード２１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図３４のような設定がなされ、無線ノードから見た中継ノード２１０２の構造は図３６のように見える。

【０１２６】

さて、中継ノード２１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード２１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャンネル＃ｘを確立し、

ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ）と、ＭＰＥＧデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップＳ２５０３，Ｓ２６０２）。送信ノード２１０１は、このサブユニットが中継ノード２１０２にあるものと解釈しているため、命令の送信先は中継ノード２１０２である。

【０１２７】

これを受信（ステップＳ２７０４）した中継ノード２１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２２１０を参照して、この命令先の実体は無線ノード２１０３にあることを認識する（ステップＳ２７０５）。

【０１２８】

よって、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャネル（＃ｙ）の確保を行い（ステップＳ２７０６）、さらにＩＳＯ信号送受信部２２０３（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２２０６（同期チャネル＃ｙを送信）を図２２の点線のように接続し、１３９４インタフェース２２０１から入力された入力データを無線区間にそのままフォワードできるようにする（ステップＳ２５０４，Ｓ２７０７）。

【０１２９】

さらに、無線ノード２１０３に対して、「無線同期チャネル＃ｙを通してデータを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形（図１９参照）で送信する（ステップＳ２５０５，Ｓ２７０８）。パケットの送信元は中継ノード２１０２である。

【０１３０】

これを受信した無線ノード２１０３は、同期チャネル＃ｙを通してデータが送られてくることを認識する（ステップＳ２８０２）。

【０１３１】

この後、送信ノード２１０１は、同期チャネル＃ｘを通して、暗号化されたＭ

ＰＥＧ映像を転送する（ステップＳ２５０６）。これを受信した中継ノード２１０２は、先に設定したようにこれをそのまま無線区間にフォワードする（ステップＳ２７０９，Ｓ２５０７，Ｓ２５０８）。

【０１３２】

このようにして、暗号化されたＭＰＥＧ映像が無線ノード２１０３に到達する（ステップＳ２８０３）が、この時点で無線ノード２１０３はこの暗号を解くための鍵を有していないため、ここから暗号を解いて、ＭＰＥＧ映像を取り出すことはできない。ここで、無線ノード２１０３は認証手続きが送信元との間で必要であることを認識する。

【０１３３】

ここで、第２の実施形態の無線区間の暗号化の方式（プロトコル）は、ＩＥＥＥ１３９４区間を含めて、第１の実施形態の暗号化方式と同様のメカニズムを持っているものとして、本実施形態の説明を行っていく。もちろん、認証方式のメカニズムは、本実施形態で示している方式に限定されるものではなく、他の種々の認証方式や暗号化方式にも適用が可能である。

【０１３４】

さて、ここで、無線ノード２１０３（のコピープロテクション処理部２３０３）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード２１０３には、上記暗号化データの送信元は中継ノード２１０２（内の映像送信サブユニット）であるように認識されているので、認証要求の宛先も、中継ノード２１０２（内の映像送信サブユニット）である。ここで、認証手続きは、無線区間向けにあらかじめ定められたものであってもよい。その際、認証要求には、無線ノード２１０３の認証フォーマットＤｃｅｒｔを付与する（ステップＳ２８０４，Ｓ２５０９）。

【０１３５】

これを受信（ステップＳ２７１０）した中継ノード２１０２は、以下の３点を認識する。

【０１３６】

１点目は、先に無線同期チャネル＃ｙを通して転送していたデータが暗号化さ

れており、ＩＥＥＥ１３９４バス区間と無線区間との両方において認証手続きと暗号鍵の取得が必要である点、２点目は、自分自身（中継ノード２１０２）が、無線ノード２１０３との認証手続きを行うべきである、という点であり、３点目は、ＩＥＥＥ１３９４バス区間（中継ノード２１０２と送信ノード２１０１）においても認証手続きを行うべきである、という点である。

【０１３７】

まず、中継ノード２１０２は、これを無線ノード２１０３から送られてきた認証要求であると解釈し、無線ノードとの認証手続きの手順を行う（ステップＳ２５０９～Ｓ２５１２）。中継ノード２１０２は、同様の認証要求を、認証要求の送信元である無線ノード２１０３に対して行おうとする。この認証要求には、中継ノードの認証フォーマットＣｃｅｒｔが含まれる（ステップＳ２７１１，Ｓ２５１０）。

【０１３８】

これを受け取った無線ノード２１０３は、これを中継ノード２１０２から送られてきた認証要求であると解釈する（ステップＳ２８０５）。その後、この認証鍵の交換に必要な残りの手続きとして、無線ノード２１０３は、認証要求の中継ノード２１０２に対して認証手続きパケットを送信する（ステップＳ２５１１）。この認証手続きパケットには、鍵交換初期値、署名等が含まれている（ステップＳ２８０６）。

【０１３９】

これと同様の手続きが中継ノード２１０１→無線ノード２１０３の方向に対しても行われる（ステップＳ２５１２，Ｓ２７１３，Ｓ２８０７）。

【０１４０】

この認証手続きパケットを受信した中継ノード２１０２および無線ノード２１０３は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマット型が正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Ｋａｕｔｈ２を導き出す。この共通の認証鍵Ｋａｕｔｈ２は、中継ノード１０２と無線ノード１０３との間で共通に持つ鍵で、この鍵Ｋａｕｔｈ２を、この両者以外の他人に知られることな

く共有することがこの時点でできるようになる（ステップＳ２７１４，Ｓ２７１５，Ｓ２８０８）。

【０１４１】

以上は、無線区間における認証手続きである。同様の認証手続きが、ＩＥＥＥ１３９４バス区間においても行われる。具体的には、中継ノード２１０２のＩＥＥＥ１３９４コピープロテクション処理部２２０８（認証フォーマットＢｃｅｒｔを持っている）と、送信ノード２１０１のコピープロテクション処理部２４０３（認証フォーマットＡｃｅｒｔを持っている）との間で行われる。手順としては、無線区間で行われた認証手続きと同様の手続きである（ステップＳ２５１３～Ｓ２５１６，Ｓ２６０４～Ｓ２６０９，Ｓ２７１７～Ｓ２７２１）。このようにして、送信ノード２１０１と中継ノード２１０２との間で共通の認証鍵ｋａｕｔｈ１を共有することになる。

【０１４２】

このように、無線区間、ＩＥＥＥ１３９４区間のそれぞれにおいて認証手続きが行われる。おのおのが終了すると、第１の実施形態と同様に、送信ノード２１０１と中継ノード２１０２との間でコンテンツキーＫ１が、中継ノード２１０２と無線ノード２１０３との間でコンテンツキーＫ２がそれぞれ共有されることになる。ここで、これ以外のノードには、これらのコンテンツキーの値は明らかになっていない。

【０１４３】

ここで、送信ノード１０１が、送信するＭＰＥＧ映像を、コンテンツキーＫ１を使って、暗号化部２４０５にて暗号化し（ステップＳ２６１０）、これを１３９４バスの同期チャネル＃ｘを通して中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に対して送信する（ステップＳ２５１７，Ｓ２６１１）。

【０１４４】

中継ノード２１０２は、送信ノード２１０１から同期チャネル＃ｘを通して送られてくる、コンテンツキーＫ１で暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部２２０３にて受信すると、これを暗号復号化部２２０４に転送する（ステ

ップＳ２５１７，Ｓ２７２２）。この暗号復号化部２２０４では、先にＩＥＥＥ１３９４区間でやり取りしたコンテンツキーＫ１の値をＩＥＥＥ１３９４コピープロテクション処理部２２０８からもらい、暗号の復号化を行う（ステップＳ２５１８，Ｓ２７２３）。こうして取り出したＭＰＥＧ映像を、今度は暗号化部２２０５に転送し、これも先に無線区間でやり直したコンテンツキーＫ２の値を使って暗号化し（ステップＳ２５１９，Ｓ２７２４）、無線ＩＳＯ信号送受信部２２０６を通して、無線同期チャネル＃ｙに送信する（ステップＳ２５２０，Ｓ２７２５）。

【０１４５】

これを受信（ステップＳ２８１０）した無線ノード２１０３は、これを先に送られてきたＫａｕｔｈ２を使ってコンテンツキーＫ２の値を導き出し、このキーＫ２の値を使ってＭＰＥＧ映像の値を復号化する（ステップＳ２８１１）。復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部２３０６にて復号化され（ステップＳ２８１２）、これをディスプレイ部２３０７にて再生する（ステップＳ２８１３）。

【０１４６】

このように、ＩＥＥＥ１３９４バスと無線網のと間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送が可能になる。

【０１４７】

もちろん、中継ノード２１０２の「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部２２０４と暗号化部２２０５との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のＬＳＩにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）す

ることが実質的に不可能になるため、このような対策を行っておくことが有益である。

【０１４８】

（第３の実施形態）

次に、第３の実施形態について説明する。

【０１４９】

第３の実施形態では、ＩＥＥＥ１３９４上において、ＨＡＶｉ規格（Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｏｆ ｔｈｅ Ｈｏｍｅ Ａｕｄｉｏ／Ｖｉｄｉｏ Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ（ＨＡＶｉ） Ａｒｃｈｉｔｅｃｔｕｒｅ）等に代表される、ＡＶ／Ｃの上位レイヤに相当するＡＶ機器制御ソフトウェアが稼働している場合における実施形態である。

【０１５０】

図３７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１５１】

図３８に、送信ノード４１０１の内部構造の一例を示す。これも第１の実施形態の場合とほぼ同様であるが、ＩＥＥＥ１２１２レジスタ４４０７を強調のため、追加記述している。ＩＥＥＥ１２１２レジスタ４４０７には、送信ノード４１０１の属性、例えば「どのベンダの製品かを示す情報、例えばＶＴＲやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置ＵＲＬ、制御アイコン、コマンド一覧」等の情報が含まれる。

【０１５２】

次に、図３９に、中継ノード４１０２の内部構造の一例を示す。中継ノード４１０２も、第１の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なＩＥＥＥ１２１２レジスタ４２１３を１３９４バス構成認識部４２０６内に特に記した点と、ＨＡＶｉ処理部４２１２を持つ点が第１の実施形態と異なる。ＨＡＶｉ処理部４２１２には、いわゆるＨＡＶｉバイトコードの処理を行う仮想マシン（ＶＭ）が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成

部４２０７が持つ。

【０１５３】

次に、図４０に、無線ノード４１０３の内部構造の一例を示す。これについても、第１の実施形態の場合と基本的には同様である。

【０１５４】

次に、ＨＡＶｉ環境における、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図４１／図４２（全体のシーケンス例）、図４３／図４４（送信ノード４１０１のフローチャート例）、図４５／図４６／図４７（中継ノード４１０２のフローチャート例）、図４８／図４９（無線ノード４１０３のフローチャート例）を参照しながら説明する。

【０１５５】

まず、無線ノード４１０３は、自分の構成情報を中継ノード４１０２に通知する（ステップＳ４５０１）。このとき、これらの構成情報は、ＩＥＥＥ１２１２レジスタ形式の情報として中継ノード４１０１に送付するものとする。すなわち、中継ノード４１０２が、無線ノード４１０３に対して「ＩＥＥＥ１２１２で規定されるＣＳＲ（コマンド・ステータスレジスタ）空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード４１０３が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード４１０３が持っている認証フォーマットをＢｃｅｒｔとする。

【０１５６】

これを受信した中継ノード４１０２は、無線ノード４１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ４７０１）。中継ノード４１０２は、無線ノード４１０１がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継ノード４１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ４５０２）。具体的には、自身のＩＥＥＥ１２１２レジスタに「

自分はＭＰＥＧデコード／ディスプレイ機能を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード４１０１等のＩＥＥＥ１３９４に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

【０１５７】

そのために、中継ノード４１０２は、代理テーブル４２０８を持つ。代理テーブル４２０８は、図５０／図５１のように、中継ノード４１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１５８】

ここでは、図５０のように、無線ノード４１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ４７０２，Ｓ４７０３）。

【０１５９】

以上と逆の手続きがＩＥＥＥ１３９４バス４１０４上の送信ノード４１０１の代理登録を無線区間側に対してみせる形で行われる（ステップＳ４５０３，Ｓ４５０４）。すなわち、送信ノード４１０１のＩＥＥＥ１２１２レジスタ４４０７に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード４１０２が読み込む（ステップＳ４６０１，Ｓ４７０４）。この送信ノード４１０１の機能を、中継ノード４１０２の機能として、代理して無線区間側のＩＥＥＥ１２１２相当機能（無線区間側のＣＳＲ空間）に反映し、無線ノード４１０３側には、上記映像送信機能、およびパネル機能が中継ノード４１０２の機能であるものとして認識してもらう。この対応関係を、代理テーブル４２０８に図５１のように反映する（ステップＳ４７０５）。

【０１６０】

このようにして代理テーブル４２０８は、図５０／図５１のように構成される。また、送信ノード４１０１から見た中継ノード４１０２の内部構造を図５２に、無線ノード４１０３から見た中継ノード４１０２の内部構造を図５３に、それ

ぞれ示す。

【０１６１】

なお、この時点で、ステップＳ４５０３の送信ノード構成情報の中に、送信ノード４１０１を制御するためのＨＡＶｉのバイトコードが含まれており、中継ノード４１０２は送信ノード４１０１の代理サーバ、すなわちＤＣＭ（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード４１０２のＨＡＶｉ処理部４２１２内の仮想マシン上で稼働することになる。

【０１６２】

さて、中継ノード４１０２にパネル機能があるものと認識した無線ノード４１０３は、中継ノード４１０２の（パネルサブユニット）に対して、パネルの表示要求のコマンドを送出する（ステップＳ４５０５，Ｓ４８０２）。これを受信（ステップＳ４７０６）した中継ノード４１０２は、代理テーブル４２０８を参照し、このパネル機能の実体が送信ノード４１０１に存在していることを認識し、前記パネル表示要求コマンドを送信ノード４１０１に対してフォワードする（ステップＳ４５０６，Ｓ４７０７）。

【０１６３】

これを受信（ステップＳ４６０１）した送信ノード４１０１は、ＡＶ／Ｃプロトコルにてパネル応答（つまり、制御画面の送信）を行う。送信先は、中継ノード４１０２である（ステップＳ４６０３，Ｓ４５０７）。これを受信（ステップＳ４７０８）した中継ノード４１０２は、代理テーブル４２０８を参照して、これを無線ノード４１０３にフォワードする（ステップＳ４７０９，Ｓ４５０８，Ｓ４８０３）。

【０１６４】

ここで、図５４に、無線ノード４１０３に送られてきた制御画面の一例を示す。この制御画面（パネル）では、６つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン１」、「ボタン２」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン１が押されました」というコマンドの形で、パネルの送信元に送られる仕組みとなっているもの

とする。

【０１６５】

さて、無線ノード４１０３は、中継ノード４１０２が提供していると認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード４１０１）、無線ノード制御パケットを使って（ステップＳ４５０９）、映像を流すための無線同期チャネル＃ｙを確保し、このチャネルを中継ノード４１０２の映像送信サブユニットに接続するためのコマンドを中継ノード４１０２に対して発行する（ステップＳ４８０４）。これを受信した中継ノード４１０２は、代理テーブル４２０８を参照して、実際にこのＡＶ／Ｃコマンドが発行されるべきノード（送信ノード４１９１）を確認し、ＩＥＥＥ1.３９４バス上に必要な帯域を確保するとともに（同期チャネル＃ｘ）、内部のＩＳＯ信号送受信部４２０４を設定して、ＩＥＥＥ１３９４バスの同期チャネル＃ｘと無線同期チャネル＃ｙとを相互に接続する（ステップＳ４７１０，Ｓ４７１１，Ｓ４７１２，Ｓ４５１０）。また、中継ノード４１０２は、送信ノード４１０１に対し、同期チャネル＃ｘを映像送信サブユニットに接続するコマンドを発行する（ステップＳ４５１１，Ｓ４７１３）。これを受信（ステップＳ４６０４）した送信ノード４１０１は、映像送信サブユニットの実体である内部の映像ストリームの流れるパス（図３８で２重矢印になっている部分）をＩＥＥＥ１３９４バスの同期チャネル＃ｘに接続する。

【０１６６】

これと前後して、無線ノード４１０３のユーザは、見たい映像を選択するために図５４のパネルの中から適当な番組を選択すべく、制御画面のボタンを押す（例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード４１０２に伝達され、これは代理テーブル４２０８の参照を経て送信ノード４１０１へのコマンドに変換される（ステップＳ４８０５，Ｓ４７１４，Ｓ４７１５，Ｓ４６０５，Ｓ４５１２，Ｓ４５１３）。

【０１６７】

この後、送信ノード４１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ４５１４，Ｓ４６０６）。これは、中継ノー

ド４１０２にて中継され、無線ノード４１０３に到達する（ステップＳ４７１６）。

【０１６８】

後の手続きは、第１の実施形態の場合と同様であり、暗号化されたＭＰＥＧ映像が無線ノード４１０３に到達する（ステップＳ４８０６）が、この時点で無線ノード４１０３はこの暗号を解くための鍵を有していないため、ＭＰＥＧ映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第１の実施形態と同様であるので、ここでの詳細な説明は省略する。

【０１６９】

なお、第１の実施形態に従えば、認証は送信ノード４１０１の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能ととの間で行われると考えられるが、第３の実施形態の場合には、このような認証方式の他に、送信ノード４１０１のパネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード４１０１のパネルにデバイスＩＤが割り当てられることになる。

【０１７０】

なお、ＨＡＶｉにおいては、送信ノード４１０１から送られてくるバイトコードであるＤＣＭ等の中に、送信ノード４１０１を制御するための制御画面情報が含まれる場合がある。このようなモジュールをＤＤＩ（データドリブンインタラクション）と呼ぶ。このようなモジュールは、例えば中継ノード４１０２内のＨＡＶｉ処理部４２１２にて展開され、制御画面が生成される。本実施形態では、この制御画面（あるいは、それと同等の機能を持つ制御画面）を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部４２０７が、このＤＤＩに含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる）、パネルとしてこの制御画面を再構成し、無線区間に「パネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル４２０８には、このパネルと、ＤＤＩで生成されるべきＨＡＶｉやＡＶ／Ｃのコマンド（中継ノード４１０

２から送信ノード４１０１に対して発行される）の対応テーブルが用意されることになる。この方法は、無線ノード４１０３内にＨＡＶｉバイトコードの仮想マシンが存在しなくても有効であるため、ＨＡＶｉ仮想マシンを持たない無線ノード４１０３から、ＨＡＶｉ機器の制御を可能とする方法である。

【０１７１】

（第４の実施形態）

次に、第４の実施形態について説明する。

【０１７２】

図５５に、本実施形態の全体構成の一例を示す。

【０１７３】

図５５に示されるように、第４の実施形態では、ある家庭のホームネットワークであるＩＥＥＥ１３９４バス６１０４と、公衆網（ここでは、一例としてインターネットとするが、電話網等でもよい）６１０５とが、ホームゲートウェイ６１０２で接続され、送信ノード６１０１と受信ノード６１０３との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット６１０５（のアクセス網部分）は、ＩＥＥＥ１３９４バス６１０４と比べて通信帯域が非常に細く、ＩＥＥＥ１３９４バスでやり取りされる映像情報（一例としてＭＰＥＧ２映像であるとする）は、帯域が足りずに通せないため、ホームゲートウェイ６１０２においてトランスコーディング、つまりＭＰＥＧ２符号からＭＰＥＧ４符号への符号変換を行った上で、伝送を行うことを考える。

【０１７４】

第４の実施形態においても、第２の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイト受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が１３９

４バス区間および無線区間のＭＰＥＧデータの暗号化転送についてのそれぞれの責任を終端する。

【０１７５】

次に、図５６に、送信ノード６１０１の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【０１７６】

次に、図５７に、ホームゲートウェイ６１０２の内部構造の一例を示す。

【０１７７】

ホームゲートウェイ６１０２の基本的な構成は、無線インタフェースではなくインターネットインタフェース６２０２を有している点、代理サブユニット構成部ではなく代理ホームページ作成部６２１０を有している点、ホームページの作成・蓄積部６２１１を有している点、暗号復号化部６２０４と暗号化部６２０５との間にＭＰＥＧ２／ＭＰＥＧ４変換部６２１４を有している点を除くと、第２の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【０１７８】

ホームゲートウェイ６１０２は、インターネット側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では、送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。送信ノード６１０１が提供しているサービス（本実施形態の場合、映像送信サービス）には、ホームゲートウェイ６１０２が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード６１０３からは、送信ノード６１０１のサービスは、ホームゲートウェイ６１０２のホームページを介して見えるため、これをホームゲートウェイ６１０２が提供するＩＰ（インターネット）上のサービスとして解釈されてもよい。

【０１７９】

また、ホームゲートウェイ６１０２は、第２の実施形態と同様に、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ２映像データ）をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクショ

ンに関する手続きがＩＥＥＥ１３９４バス区間とインターネット区間との両方について、このホームゲートウェイにおいて終端されている。ＩＥＥＥ１３９４バス側については、認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部６２０８に、インターネット区間側については、認証フォーマットＣｃｅｒｔをインターネット側コピープロテクション処理部６２１２にそれぞれ持ち、ＩＥＥＥ１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号送受信部６２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ２映像をＭＰＥＧ２／ＭＰＥＧ４変換部６２１４にてトランスコード→ＭＰＥＧ４映像を暗号化部６２０５にて再暗号化→ＡＶ信号送受信部６２０６にてインターネット側に送信、というプロセスを踏む。

ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１８０】

次に、図５８に、受信ノード６１０３の内部構造の一例を示す。

【０１８１】

コピープロテクション処理部６３０３がインターネット向けの認証フォーマットＤｃｅｒｔを持っている。第２の実施形態との相違点は、インタフェース（インターネットインタフェース６３０１、制御パケット送受信部６３０２、ＡＶ信号送受信部６３０４）がインターネット対応となっている点である。ここで、制御パケット送受信部６３０２はＴＣＰ、ＡＶ信号送受信部６３９４はＵＤＰのトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

【０１８２】

次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図５９／図６０（全体のシーケンス例）、図６１（送信ノード６１０３のフローチャート例）、図６２／図６３（ホームゲートウェイ６１０２のフロ

ーチャート例）、図６４（受信ノード６１０３のフローチャート例）を参照しながら説明する。

【０１８３】

まず、ホームゲートウェイ６１０２は、送信ノード６１０１のＩＥＥＥ１２１２レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する（ステップＳ６５０１，Ｓ６６０１，Ｓ６７０１，Ｓ６５０２，Ｓ６６０２，Ｓ６７０２）。これを通して、ホームゲートウェイ６１０２は、送信ノード６１０１が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【０１８４】

これを受けて、ホームゲートウェイ６１０２は、送信ノード６１０１を遠隔制御するためのホームページを作成する（ステップＳ６５０３）。基本的には、送信ノード６１０１が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード６１０１のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部６２１０内の変換テーブルに対応の一覧が記述される。例えば、送信ノード６１０１のパネルサブユニットに「再生」とかかれているボタンが存在する場合には、該ホームページにも「再生」とかかれているボタンを用意して、この関係を前記変換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ６１０２から送信ノード６１０１のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図６５（ａ）に送信ノード６１０１のパネルサブユニットの持つパネルの一例を、図６５（ｂ）にホームゲートウェイ６１０２の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【０１８５】

さて、インターネット上の受信ノード６１０３は、インターネットを介してこのホームゲートウェイ６２０１にアクセスし、送信ノード６１０１の制御画面を含むホームページを要求し、このホームページが送付される（ステップＳ６５０４，Ｓ６８０１，Ｓ６７０３）。これを見て、受信ノード６１０３のユーザは、

画面上の映像送信を要求するボタン（例えば、図６５（ｂ）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」、というインタラクションが、インターネット経由でホームゲートウェイにＨＴＴＰを通じて通知される（ステップＳ６５０５，Ｓ６８０２，Ｓ６７０４）。

【０１８６】

これを受信したホームゲートウェイ６１０２は、受信した命令を解釈し、その命令が、自らがホームページを通じて代理サービスを行っている送信ノード６１０１の映像送信サブユニット、およびパネルサブユニットに対する命令であることを認識する。よって、ＩＥＥＥ１３９４上に映像送信のための同期チャネル＃ｘを確保し、この同期チャネルを送信ノードの映像送信サブユニットと接続する手続きを行う。また、送信ノード６１０１のパネルサブユニットに対して、「再生」に該当するボタンを押すことを意味するコマンドを送信する（ステップＳ６５０６，Ｓ６７０５）。

【０１８７】

これを受信した送信ノード６１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ２映像を送出する（ステップＳ６５０７）。第２の実施形態においては、中継ノードは送られてきたＭＰＥＧ映像をそのまま無線ノードにフォワーディングしていたが、本第４の実施形態においては、内部でＭＰＥＧ４からＭＰＥＧ２にトランスコードしなくてはいけないため、ＭＰＥＧ２映像はホームゲートウェイ６１０２内にて復号化される必要がある。ところが、この時点でホームゲートウェイ６１０２は、この暗号を解くための鍵を有していないため、ここから暗号を解いて、ＭＰＥＧ２映像を取り出すことはできない。ここで、ホームゲートウェイ６１０２は、認証手続きが送信元との間で必要であることを認識する（ステップＳ６５０８，Ｓ６７０６）。

【０１８８】

しかしながら、ホームゲートウェイ６１０２は、これから受信ノード６１０３に転送しようとしているデータが、認証手続きが必要なコンテンツであることを認識し、まず、受信ノード６１０３が信頼に足るノードであるのかをまず確かめるべく、ホームゲートウェイ６１０２と受信ノード６１０３との間で認証手続き

を行う（ステップＳ６７０７，Ｓ６５０９，Ｓ６５１０）。このようにすることにより、未然に悪意ユーザに対するコンテンツの送信を、いずれの符号化形式、あるいはいずれの接続ネットワークのいかんを問わず、行うことができる。

【０１８９】

この認証・鍵交換手続きは、第２の実施形態のＩＥＥＥ１３９４上の認証・鍵交換手続きをインターネット上で行ってもよいし、ＩＳＰＥＣ等のインターネット上で定められた認証・鍵交換手続きにてこれを行ってもよい。

【０１９０】

具体的には、ホームゲートウェイ６１０２は、受信ノード６１０３巻の認証手続きが終了すると、受信ノード６１０３が信頼に足るノードであることを確認し、映像を送信しても大丈夫であると判断し、次に自身と送信ノード６１０１との認証手続きにはいる。具体的には、ホームゲートウェイ６１０２は、送信ノード６１０１に対して、認証要求を送信する（ステップＳ６５１１，Ｓ６７０９，Ｓ６６０５）。これに引き続き、ホームゲートウェイ６１０２と送信ノード６１０１との間において、認証手続きが行われる（ステップＳ６５１２，Ｓ６７１０，Ｓ６６０６）。この認証手続きについても、これまでの実施形態で行われてきた認証手続きと同様の手続きが行われてもよい。

【０１９１】

以上のようにして、認証が終了したノード間において、コンテンツの暗号化を行う鍵についての情報が共有される。送信ノード２１０１とホームゲートウェイ６１０２との間でコンテンツキーＫ１が、ホームゲートウェイ６１０２と受信ノード６１０３との間でコンテンツキーＫ２がそれぞれ共有されることになる。

【０１９２】

ここで、送信ノード６１０１が、送信するＭＰＥＧ２映像を、コンテンツキーＫ１を使って、暗号化部６４０５にて暗号化し（ステップＳ６６０７）、これを１３９４バスの同期チャネル＃ｘを通してホームゲートウェイ６１０２に対して送信する（ステップＳ６６０８，Ｓ６５１３）。

【０１９３】

ホームゲートウェイ６１０２は、送信ノード６１０１から同期チャネル＃ｘを

通して送られてくる、コンテンツキーＫ１で暗号化されたＭＰＥＧ２映像を、ＩＳＯ信号送受信部６２０３にて受信すると、これを暗号復号化部６２０４に転送する（ステップＳ６７１１）。この暗号復号化部６２０４では、先にＩＥＥＥ１３９４区間でやり取りしたコンテンツキーＫ１の値をＩＥＥＥ１３９４コピープロテクション処理部６２０８からもらい、暗号の復号化を行う（ステップＳ６５１４，Ｓ６７１２）。こうして取り出したＭＰＥＧ２映像を、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４にて符号変換を行い、インターネットでも送信しうる帯域に帯域圧縮を行う（ステップＳ６５１５，Ｓ６７１３）。ＭＰＥＧ４符号化されたデータは、暗号化部６２０５に転送され、これも先にインターネット区間でやり取りしたコンテンツキーＫ２の値を使って暗号化し（ステップＳ６５１６，Ｓ６７１４）、ＡＶ信号送受信部６２０６を通して、インターネット側に送信する（ステップＳ６５１７，Ｓ６７１５）。

【０１９４】

ここで、ホームゲートウェイ６１０２の暗号復号化部６２０４からＭＰＥＧ２／ＭＰＥＧ４変換部６２１４を経由して、暗号化部６２０５にかけては生のＭＰＥＧ２またはＭＰＥＧ４データが流れることになるので、不正コピーがなされないように保護がなされている（例えば、暗号化復号化部とＭＰＥＧ２／ＭＰＥＧ４変換部、暗号化部を一体のＬＳＩにするなど）のが望ましい。

【０１９５】

さて、これを受信（ステップＳ６８０５）した受信ノード６１０３は、これを先に作成した鍵情報（Ｋ２）を使ってＭＰＥＧ４映像の値を復号化する（ステップＳ６８０６）。復号化されたＭＰＥＧ４データは、ＭＰＥＧデコード部６３０６にて復号化され（ステップＳ６８０７）、これをディスプレイ部６３０７にて再生する（ステップＳ６８０８）。

【０１９６】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで

暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０１９７】

（第５の実施形態）

次に、第５の実施形態について説明する。

【０１９８】

第４の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第５の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【０１９９】

図６６に、本実施形態の全体構成図を示す。

【０２００】

図６６に示されるように、第５の実施形態では、２つの家庭網８１０５，８１０７が公衆網（ここでは、一例としてインターネットとするが、Ｂ－ＩＳＤＮ等でもよい）８１０６にて接続されている。第１の家庭網８１０５上の送信ノード８１０１から、コピープロテクションを考慮した形で、ＡＶコンテンツを第２の家庭網８１０７上の受信ノード８１０４に送信する。ここで、第４の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【０２０１】

第５の実施形態においては、第１の実施形態の中継ノードと同様に、ホームゲートウェイ８１０２，８１０３にて、ＩＥＥＥ１３９４バス８１０５，８１０７上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ８１０２，８１０３は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【０２０２】

送信ノード８１０１や受信ノード８１０４は、基本的には第４の実施形態と同様の構成である。

【０２０３】

図６７に、ホームゲートウェイ８１０２，８１０３の内部構造の一例を示す。

ホームゲートウェイ８１０２の基本的な構成は、コピープロテクションを終端しない点（これは、第１の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第１の実施形態の中継ノードと同様）を除き、第４の実施形態のホームゲートウェイの構成とほぼ同様である。

【０２０４】

図６８に、全体のシーケンスの一例を示す。

【０２０５】

ここでは、第２の家庭網８１０７のユーザが、ホームゲートウェイ８１０３の制御画面を使って、送信ノード８１０１のコンテンツを、インターネット８１０６を介して受信ノード８１０４に配信させる場合を考える。

【０２０６】

まず、第４の実施形態と同様に、ステップＳ８３０１の構成認識と、ステップＳ８３０２の送信ノード制御用ホームページ作成が行われる。

【０２０７】

第２の家庭網８１０７のユーザは、ホームゲートウェイ８１０３を操作し、ホームゲートウェイ８１０２から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップＳ８３０３）。また、例えば図６９に例示するような受信ノード８１０４の制御画面も同時に開く。そこで、図６９のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ８１０３に映像配信を命令する（ステップＳ８３０４）。

【０２０８】

すると、第４の実施形態と同様に、映像送信要求がホームゲートウェイ８１０２に（インターネットコマンドとして）発行され（ステップＳ８３０５）、これ

がホームゲートウェイ８１０２にてＡＶ／Ｃプロトコルコマンドに翻訳され、送信ノード８１０１から受信ノード８１０４間の通信パス（ＩＥＥＥ１３９４バス８１０５上の同期チャネル＃ｘ、インターネット上のコネクション、ＩＥＥＥ１３９４バス上の同期チャネル＃ｙ）が設定される（ステップＳ８３０６，Ｓ８３０７）。この上を、暗号鍵Ｋで暗号化されたＭＰＥＧ２映像が配信される（ステップＳ８３０８～Ｓ８３１０）。

【０２０９】

第１の実施形態と同様に、これを受信した受信ノード８１０６は、送信元に認証要求を発行する（ステップＳ８３１１）。受信ノード８１０４は、この映像はホームゲートウェイ８１０３から配信されていると解釈しているため、この認証要求はホームゲートウェイ８１０３に対して行われる。

【０２１０】

ホームゲートウェイ８１０３は、第４の実施形態と同様に、内部の変換テーブル８２１１を参照して、これをホームゲートウェイ８１０２にフォワードする。これは、ホームゲートウェイ８１０３は、映像の配信元がホームゲートウェイ８１０２であると解釈しているからである。このフォワードは、認証要求８３１１の中身を変えない形で、インターネットパケットで行われる（ステップＳ８３１２）。同様に、ホームゲートウェイ８１０２は、これを受信ノード８１０１にフォワードする（ステップＳ８３１３）。送信ノード８１０１は、これをホームゲートウェイ８１０１から発行された認証要求であると解釈する。

【０２１１】

これと同様の手順を双方向に組み、送信ノード８１０１と受信ノード８１０４間で認証手続きが行われる（ステップＳ８３１４）。この間、ホームゲートウェイは、この手続きのパケットを中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード８１０４は鍵の入手を行い、結局、暗号化されたＭＰＥＧ２映像の復号化ができるようになる。

【０２１２】

しかして、送信ノード８１０１が送信するＭＰＥＧ映像を、コンテンツキーＫを使って暗号化し、これが１３９４バスの同期チェネル＃ｘ、ホームゲートウェ

イ８１０２、公衆網、ホームゲートウェイ８１０３、１３９４バスの同期チェネル＃ｙという経路を辿って、受信ノード８１０３に到達する（ステップＳ８３１５～Ｓ８３１７）。そして、受信ノード８１０３では、暗号化されたＭＰＥＧ映像は、暗号鍵Ｋを使って暗号復号化され、デコードされて、再生表示される。

【０２１３】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２１４】

なお、第５の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第４の実施形態の符号化変換（例えば、ホームゲートウェイ８１０２ではＭＰＥＧ２／ＭＰＥＧ４変換、ホームゲートウェイ８１０３ではＭＰＥＧ４／ＭＰＥＧ２変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２１５】

なお、第１～第５の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合（例えば、無線ノードからＩＥＥＥ１３９４上のノードへデータ転送する場合）にも、本発明は適用可能である。

【０２１６】

また、第１～第５の実施形態において、無線ノードやＩＥＥＥ１３９４上のノードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードやＩＥＥＥ１３９４上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

【０２１７】

また、認証手続きや、鍵交換手続き（コンテンツ鍵共有手続き）は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【０２１８】

また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【０２１９】

なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０２２０】

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０２２１】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２２２】

【発明の効果】

本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係るネットワークの全体構成の一例を示す図

【図２】

送信ノードの内部構造の一例を示す図

【図３】

中継ノードの内部構造の一例を示す図

【図４】

無線ノードの内部構造の一例を示す図

【図５】

全体のシーケンスの一例を示す図

【図６】

全体のシーケンスの一例を示す図

【図７】

送信ノードの動作手順の一例を示すフローチャート

【図８】

送信ノードの動作手順の一例を示すフローチャート

【図９】

中継ノードの動作手順の一例を示すフローチャート

【図１０】

中継ノードの動作手順の一例を示すフローチャート

【図１１】

中継ノードの動作手順の一例を示すフローチャート

【図１２】

無線ノードの動作手順の一例を示すフローチャート

【図１３】

無線ノードの動作手順の一例を示すフローチャート

【図１４】

無線ノード構成情報パケットの一例を示す図

【図１５】

代理テーブルの一例を示す図

【図１６】

代理テーブルの一例を示す図

【図１７】

送信ノードから見た中継ノードの内部構造を説明するための図

【図１８】

無線ノードから見た中継ノードの内部構造を説明するための図

【図１９】

無線ノード制御パケットの一例を示す図

【図２０】

本発明の第２の実施形態に係るネットワークの全体構成の一例を示す図

【図２１】

送信ノードの内部構造の一例を示す図

【図２２】

中継ノードの内部構造の一例を示す図

【図２３】

無線ノードの内部構造の一例を示す図

【図２４】

全体のシーケンスの一例を示す図

【図２５】

全体のシーケンスの一例を示す図

【図２６】

送信ノードの動作手順の一例を示すフローチャート

【図２７】

送信ノードの動作手順の一例を示すフローチャート

【図２８】

中継ノードの動作手順の一例を示すフローチャート

【図２９】

中継ノードの動作手順の一例を示すフローチャート

【図３０】

中継ノードの動作手順の一例を示すフローチャート

【図３１】

無線ノードの動作手順の一例を示すフローチャート

【図３２】

無線ノードの動作手順の一例を示すフローチャート

【図３３】

代理テーブルの一例を示す図

【図３４】

代理テーブルの一例を示す図

【図３５】

送信ノードから見た中継ノードの内部構造を説明するための図

【図３６】

無線ノードから見た中継ノードの内部構造を説明するための図

【図３７】

本発明の第３の実施形態に係るネットワークの全体構成の一例を示す図

【図３８】

送信ノードの内部構造の一例を示す図

【図３９】

中継ノードの内部構造の一例を示す図

【図４０】

無線ノードの内部構造の一例を示す図

【図４１】

全体のシーケンスの一例を示す図

【図４２】

全体のシーケンスの一例を示す図

【図４３】

送信ノードの動作手順の一例を示すフローチャート

【図４４】

送信ノードの動作手順の一例を示すフローチャート

【図４５】

中継ノードの動作手順の一例を示すフローチャート

【図４６】

中継ノードの動作手順の一例を示すフローチャート

【図４７】

中継ノードの動作手順の一例を示すフローチャート

【図４８】

無線ノードの動作手順の一例を示すフローチャート

【図４９】

無線ノードの動作手順の一例を示すフローチャート

【図５０】

代理テーブルの一例を示す図

【図５１】

代理テーブルの一例を示す図

【図５２】

送信ノードから見た中継ノードの内部構造を説明するための図

【図５３】

無線ノードから見た中継ノードの内部構造を説明するための図

【図５４】

無線ノードに送られてきた制御画面の一例を示す図

【図５５】

本発明の第４の実施形態に係るネットワークの全体構成の一例を示す図

【図５６】

送信ノードの内部構造の一例を示す図

【図５７】

ホームゲートウェイの内部構造の一例を示す図

【図５８】

受信ノードの内部構造の一例を示す図

【図５９】

全体のシーケンスの一例を示す図

【図６０】

全体のシーケンスの一例を示す図

【図６１】

送信ノードの動作手順の一例を示すフローチャート

【図６２】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図６３】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図６４】

受信ノードの動作手順の一例を示すフローチャート

【図６５】

送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図

【図６６】

本発明の第５の実施形態に係るネットワークの全体構成の一例を示す図

【図６７】

ホームゲートウェイの内部構造の一例を示す図

【図６８】

全体のシーケンスの一例を示す図

【図６９】

制御画面の一例を示す図

【符号の説明】

１０１，２１０１，４１０１，６１０１，８１０１…送信ノード

１０２，２１０２，４１０２…中継ノード

１０３，２１０３，４１０３，６１０４…無線ノード

６１０２，８１０２，８１０３…ホームゲートウェイ

６１０３，８１０４…受信ノード

１０４，２１０４，４１０４，８１０５，８１０７…ＩＥＥＥ１３９４バス

６１０５，８１０６…公衆網

２０１，２２０１，４２０１，６２０１，８２０１…ＩＥＥＥ１３９４インタフェース

２０２，２２０２，４２０２…無線インタフェース

２０３，２２０７，４２０３，６２０７，８２０３…ＡＶ／Ｃプロトコル処理部

２０４，２２０３，４２０４，６２０３，８２０４…ＩＳＯ信号送受信部

２０５，２２０６，４２０５…無線ＩＳＯ信号送受信部

２０６，２２０９，４２０６，６２０９…１３９４バス構成認識部

２０７，２２１０，４２０７，８２０７…代理サブユニット構成部

２０８，２２１４，４２０８，６２１５…代理テーブル

２０９，２２１１，４２０９…無線区間構成認識部

２１０，４２１０，８２０９…コピープロテクション制御／フォワード部

２２０８，６２０８…ＩＥＥＥ１３９４コピープロテクション処理部

２２１２…無線区間コピープロテクション部

８２１１…変換テーブル

２１１，２２１３，４２１１…無線ノード制御パケット送受信部

２２０４，６２０４…暗号復号化部

２２０５，６２０５…暗号化部

４２１２…ＨＡＶｉ処理部

４２１３…ＩＥＥＥ１２１２レジスタ

６２０６，８２０５…ＡＶ信号送受信部

６２０２，８２０２…インターネットインタフェース

６２１０，８２０８…代理ホームページ作成部

６２１１，８２１０…ホームページ作成・蓄積部

６２１２…インターネット側プロテクション処理部

６２１３…制御パケット送受信部

６２１４…ＭＰＥＧ２／ＭＰＥＧ４変換部

６２０６…制御パケット処理信部

３０１，２３０１，４３０１…無線インタフェース

３０２，２３０２，４３０２…無線ノード制御パケット送受信部

３０３，２３０３，４３０３，６３０３…コピープロテクション処理部

３０４，２３０４，４３０４…無線ＩＳＯ信号送受信部

３０５，２３０５，４３０５，６３０５…暗号復号化部

３０６，２３０６，４３０６，６３０６…ＭＰＥＧデコード部

３０７，２３０７，４３０７，６３０７…ディスプレイ部

６３０１…インターネットインタフェース

６３０２…制御パケット送受信部

６３０４…ＡＶ信号送受信部

４０１，２４０１，４４０１，６４０１…ＩＥＥＥ１３９４インタフェース

４０２，２４０２，４４０２，６４０２…ＡＶ／Ｃプロトコル処理部

４０３，２４０３，４４０３，６４０３…コピープロテクション処理部

４０４，２４０４，４４０４，６４０４…ＩＳＯ信号送受信部

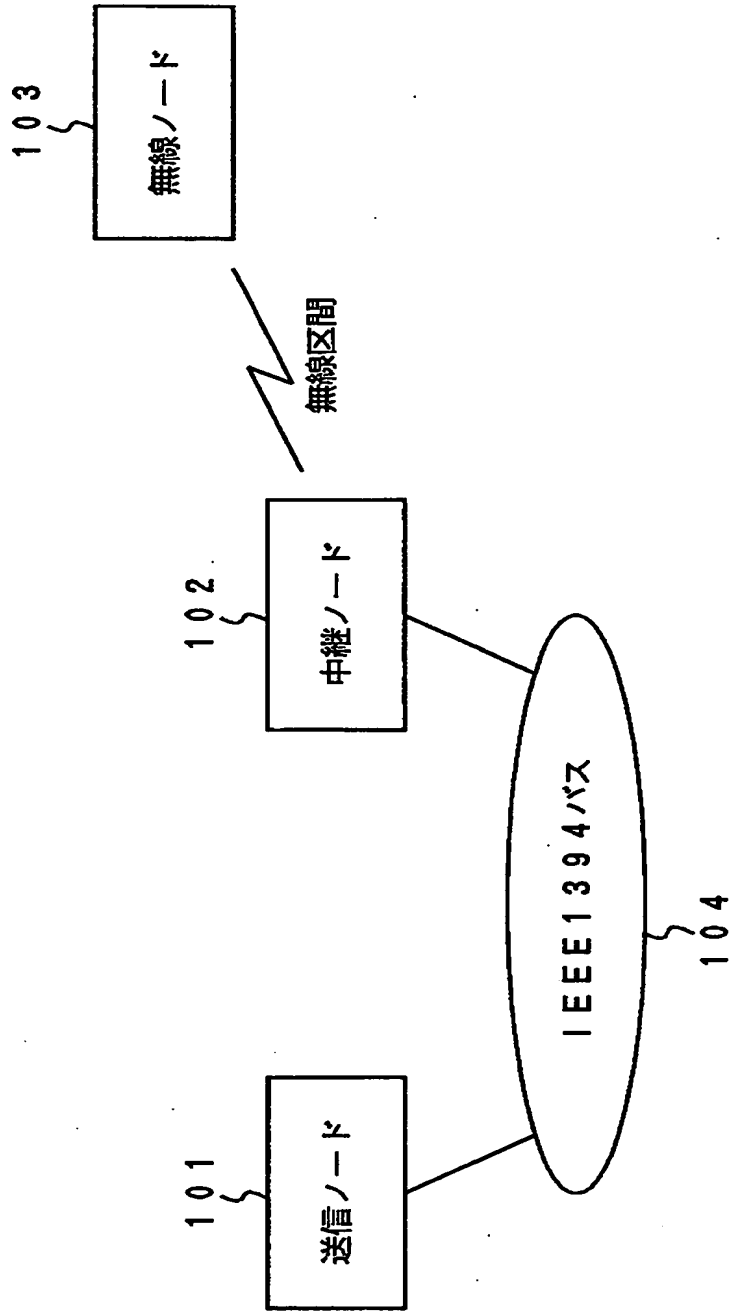
４０５，２４０５，４４０５，６４０５…暗号化部

４０６，２４０６，４４０６，６４０６…ＭＰＥＧストレージ部

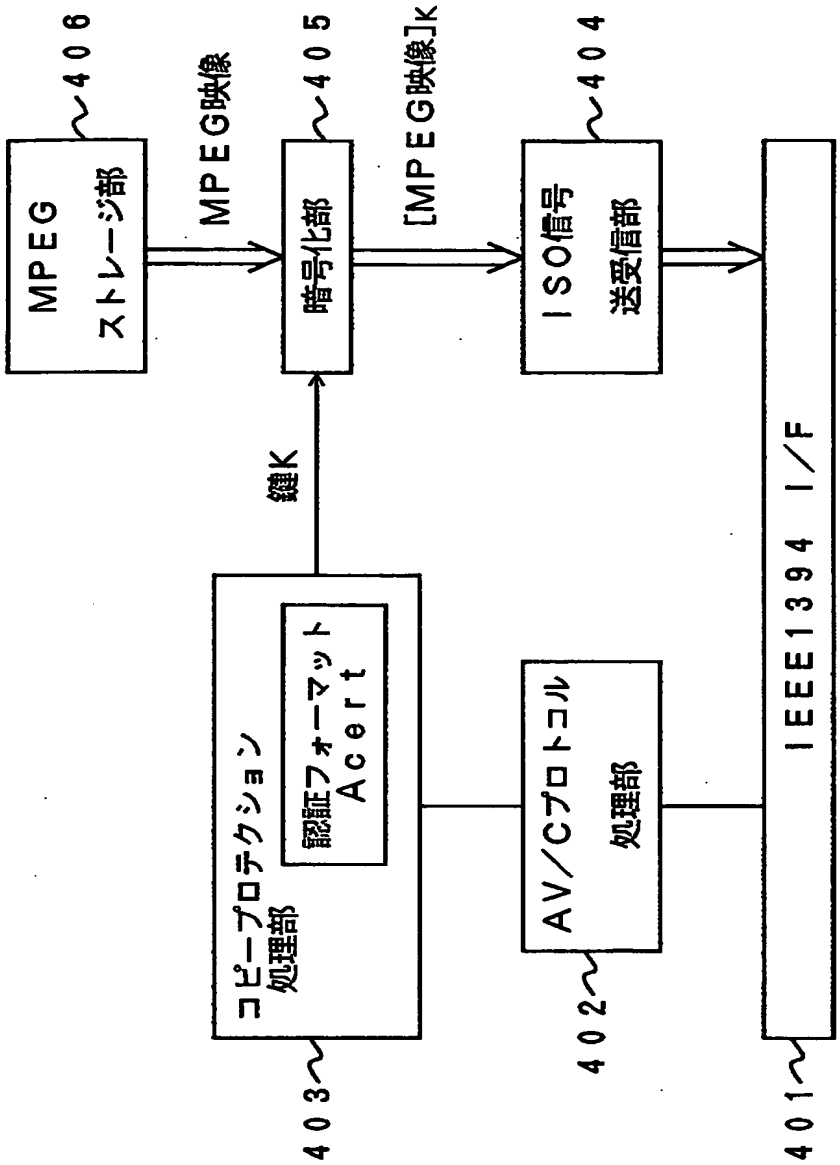
４４０７…ＩＥＥＥ１２１２レジスタ

【書類名】　図面

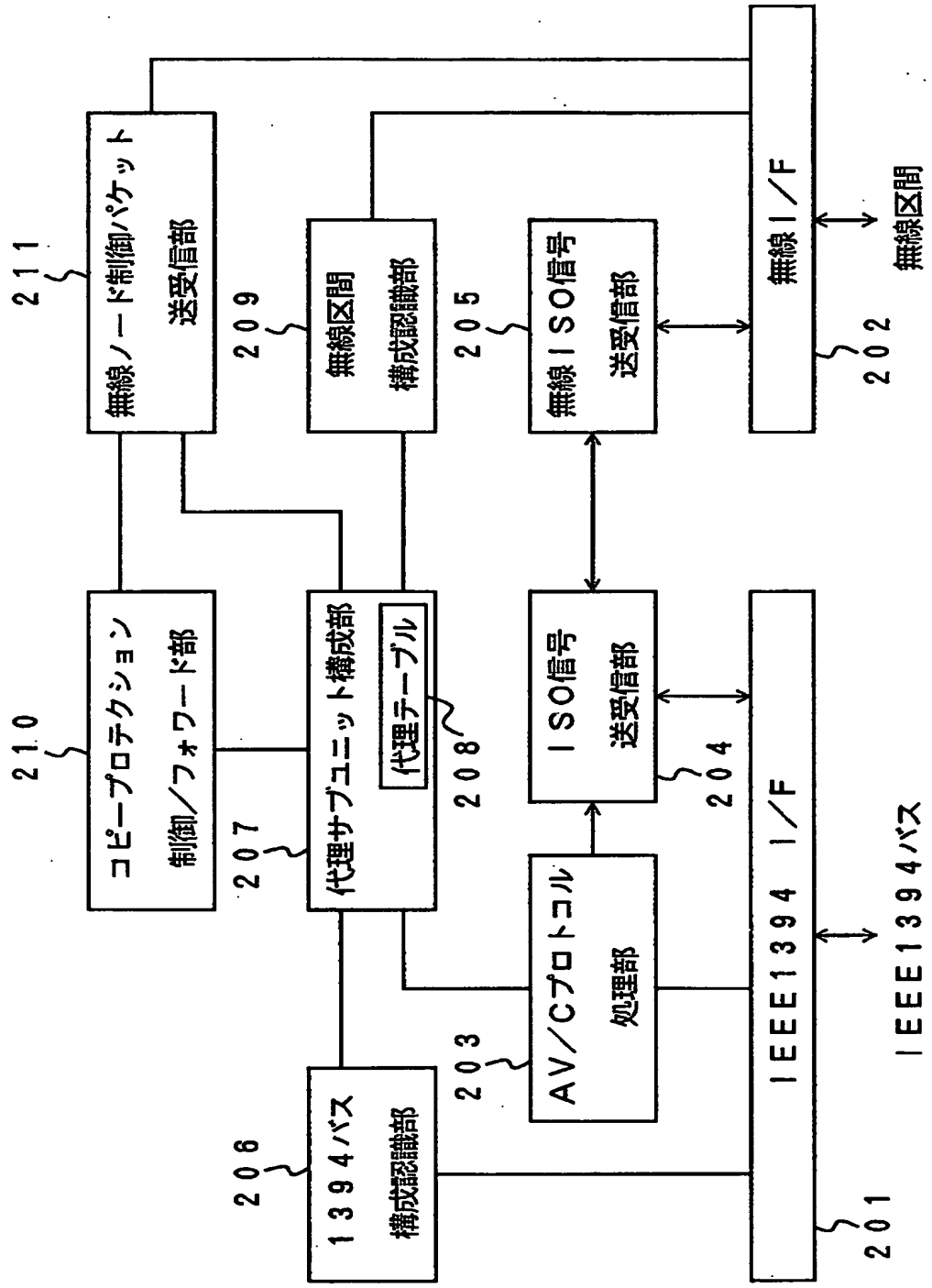
【図１】



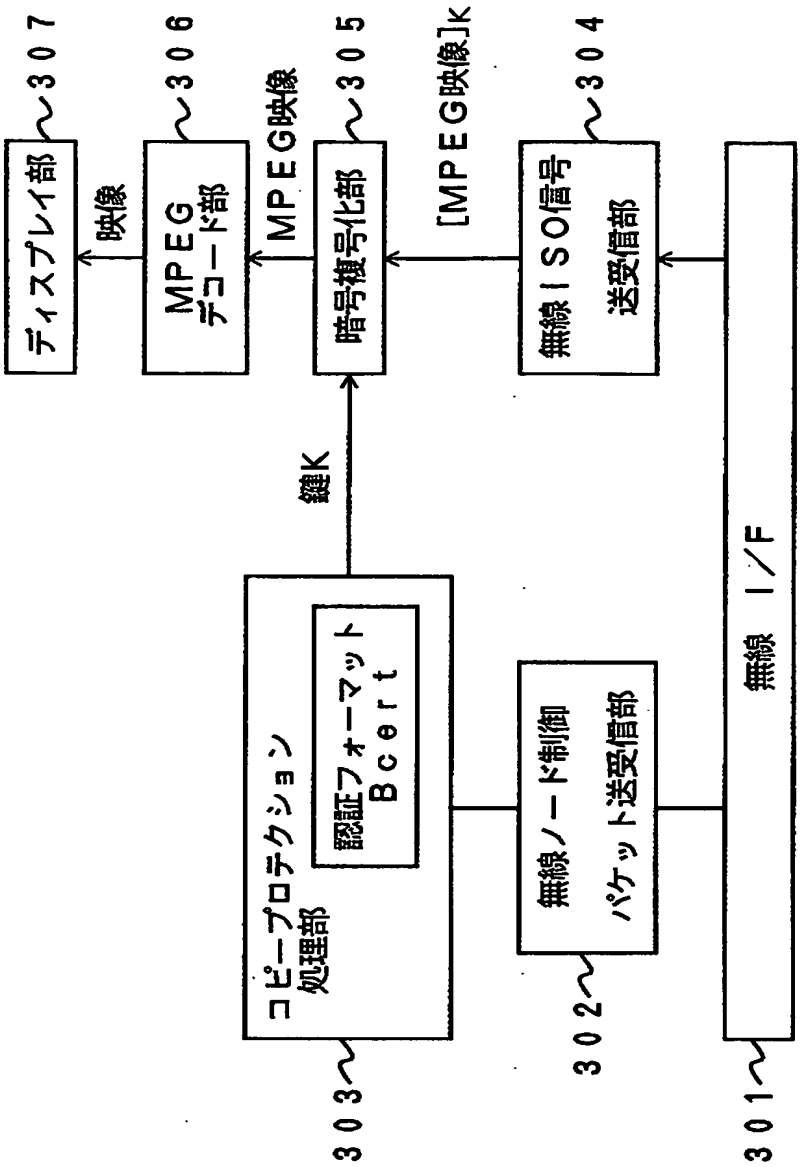
【図２】


406
MPEG
ストレージ部
MPEG映像
405
暗号化部
[MPEG映像]K
404
ISO信号
送受信部
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
403
AV/Cプロトコル
処理部
402
IEEE1394 I/F
401

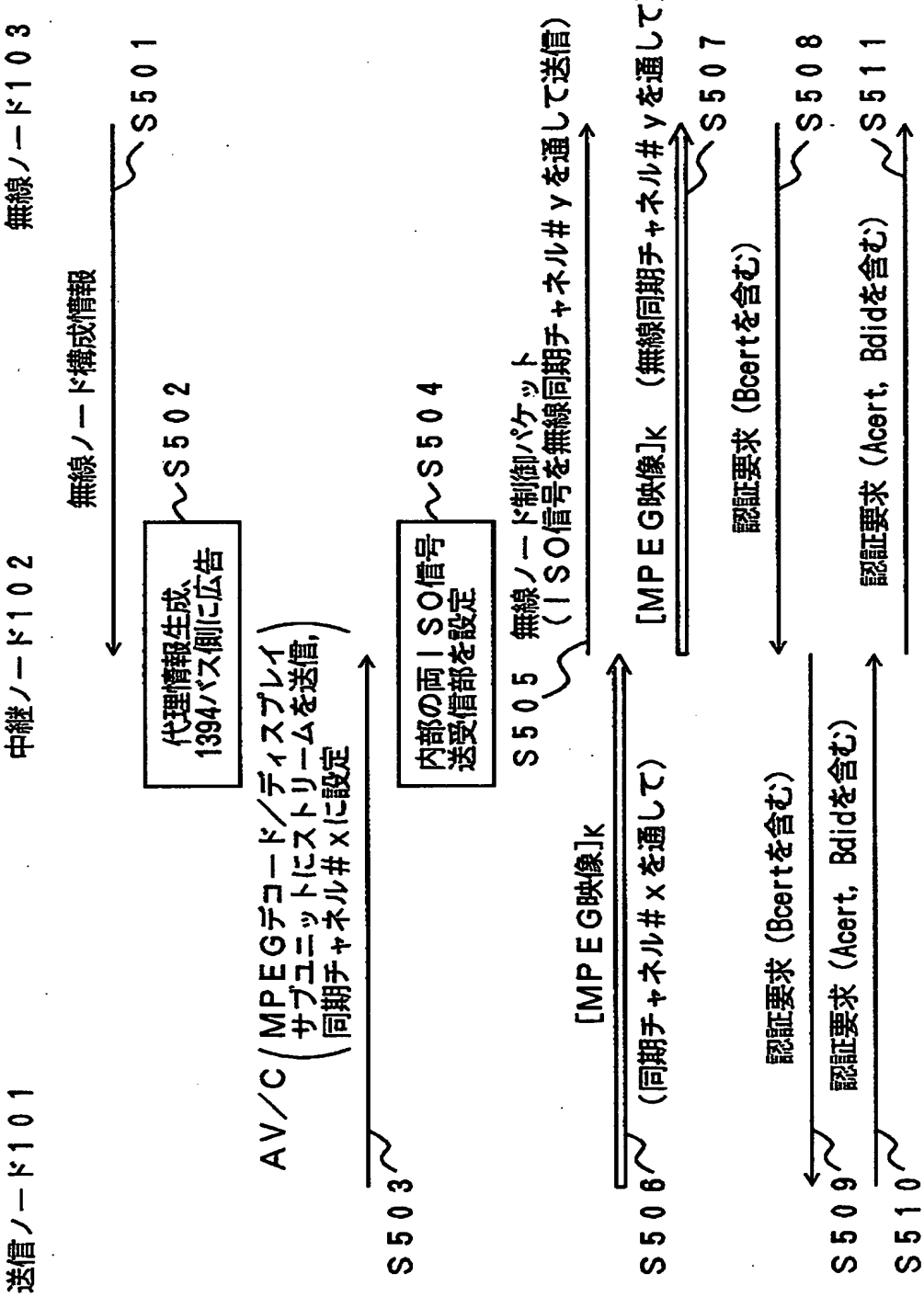
【図３】


無線ノード制御パケット
送受信部
211
無線区間
構成認識部
209
無線ＩＳＯ信号
送受信部
205
無線Ｉ／Ｆ
202
無線区間
コピープロテクション
制御／フォワード部
210
代理サブユニット構成部
代理テーブル
207
208
ＩＳＯ信号
送受信部
204
ＡＶ／Ｃプロトコル
処理部
203
ＩＥＥＥ１３９４
Ｉ／Ｆ
ＩＥＥＥ１３９４バス
１３９４バス
構成認識部
206
201

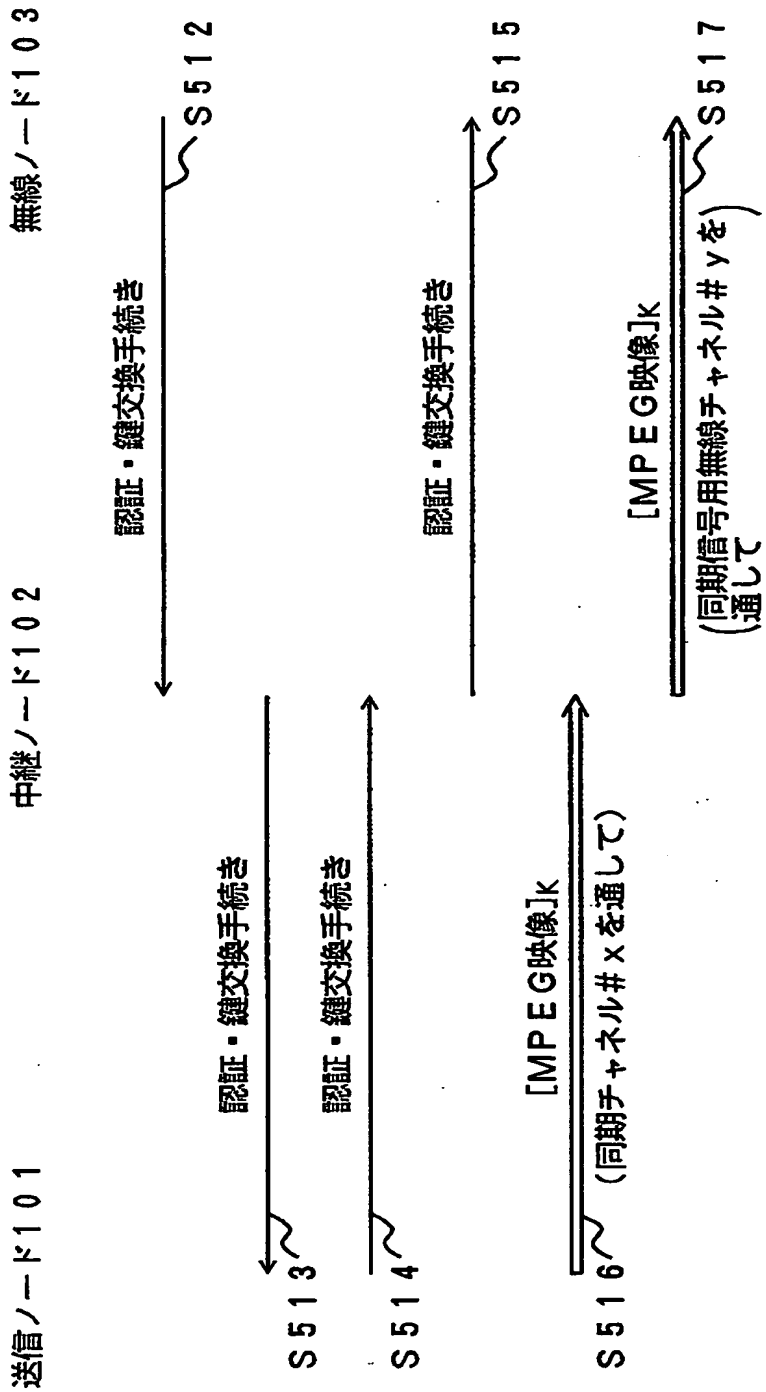
【図４】


ディスプレイ部
３０７
映像
MPEG
デコード部
３０６
MPEG映像
暗号複号化部
３０５
[MPEG映像]K
無線ISO信号
送受信部
３０４
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
３０３
無線ノード制御
パケット送受信部
３０２
無線 I／F
３０１

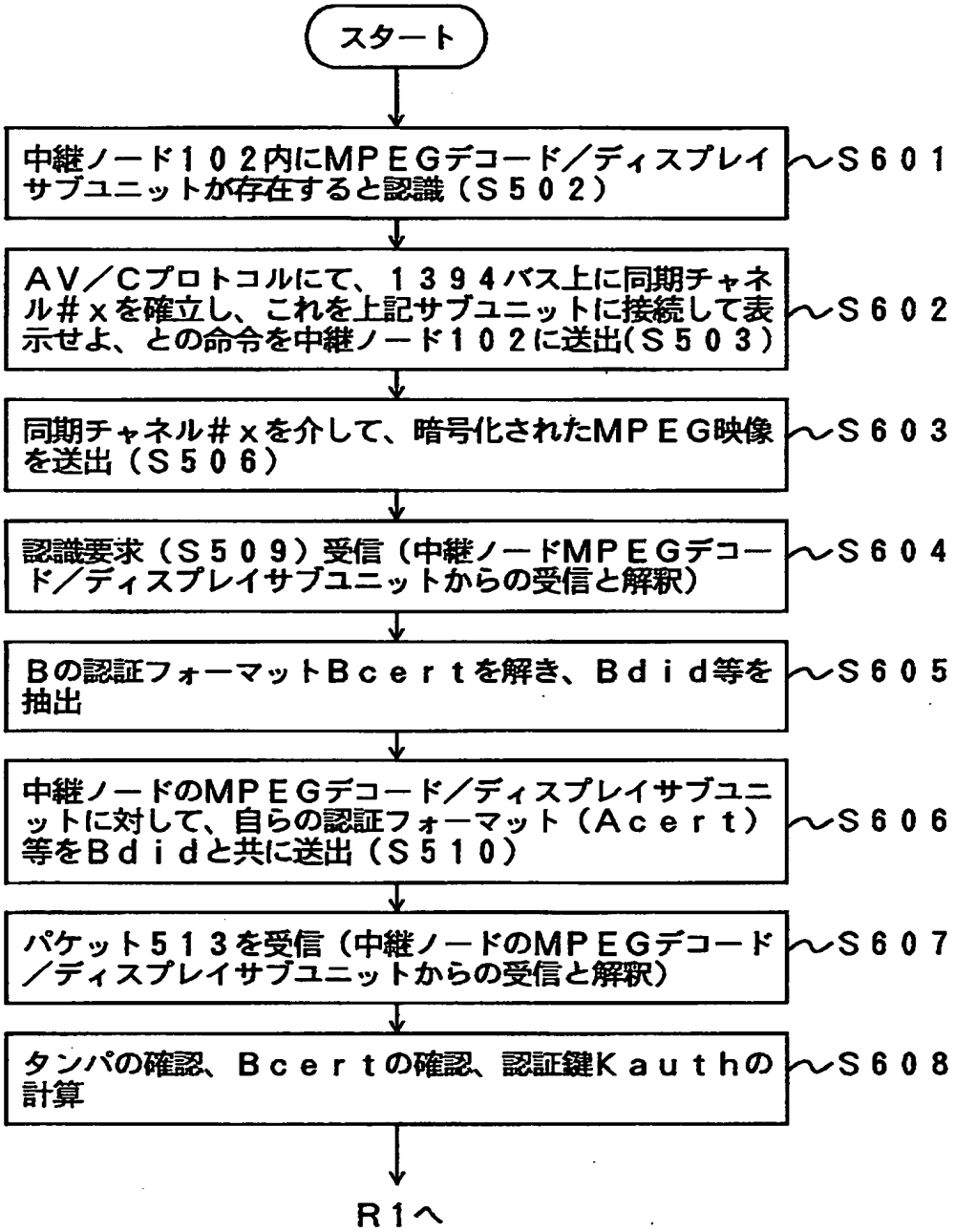
【図５】


送信ノード１０１
中継ノード１０２
無線ノード１０３
無線ノード構成情報
Ｓ５０１
代理情報生成、
1394バス側に広告
Ｓ５０２
AV／C（MPEGデコード／ディスプレイ
サブユニットにストリームを送信，
同期チャネル＃ｘに設定）
Ｓ５０３
内部の両ＩＳＯ信号
送受信部を設定
Ｓ５０４
Ｓ５０５ 無線ノード制御パケット
（ＩＳＯ信号を無線同期チャネル＃ｙを通して送信）
[ＭＰＥＧ映像]ｋ
（同期チャネル＃ｘを通して）
Ｓ５０６
[ＭＰＥＧ映像]ｋ （無線同期チャネル＃ｙを通して）
Ｓ５０７
認証要求（Bcertを含む）
Ｓ５０８
認証要求（Bcertを含む）
Ｓ５０９
認証要求（Acert，Bdidを含む）
Ｓ５１０
認証要求（Acert，Bdidを含む）
Ｓ５１１

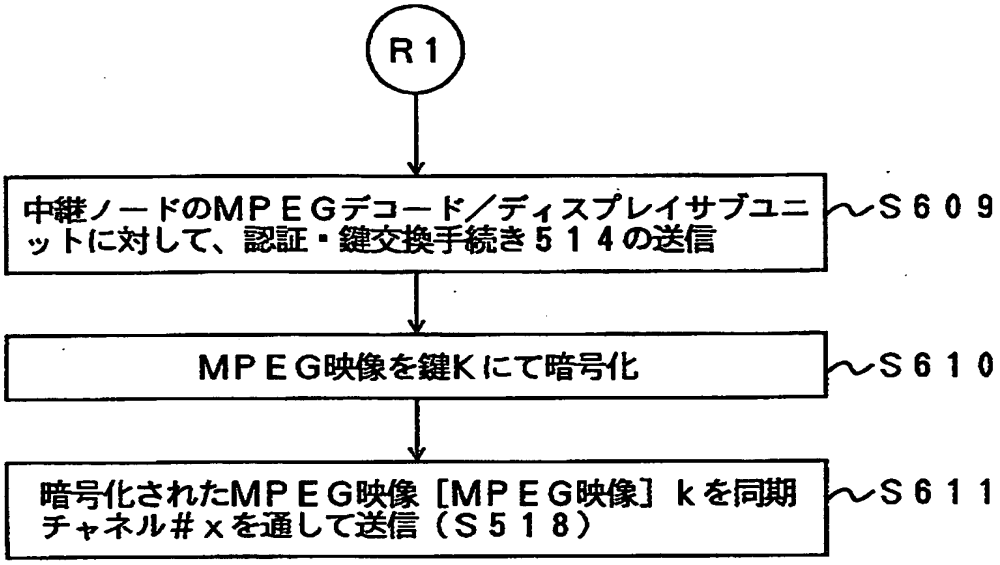
【図６】


送信ノード１０１
中継ノード１０２
無線ノード１０３
認証・鍵交換手続き
S５１２
認証・鍵交換手続き
S５１３
認証・鍵交換手続き
S５１４
認証・鍵交換手続き
S５１５
[MPEG映像]K
(同期チャネル#xを通して)
S５１６
[MPEG映像]K
(同期信号用無線チャネル#yを通して)
S５１７

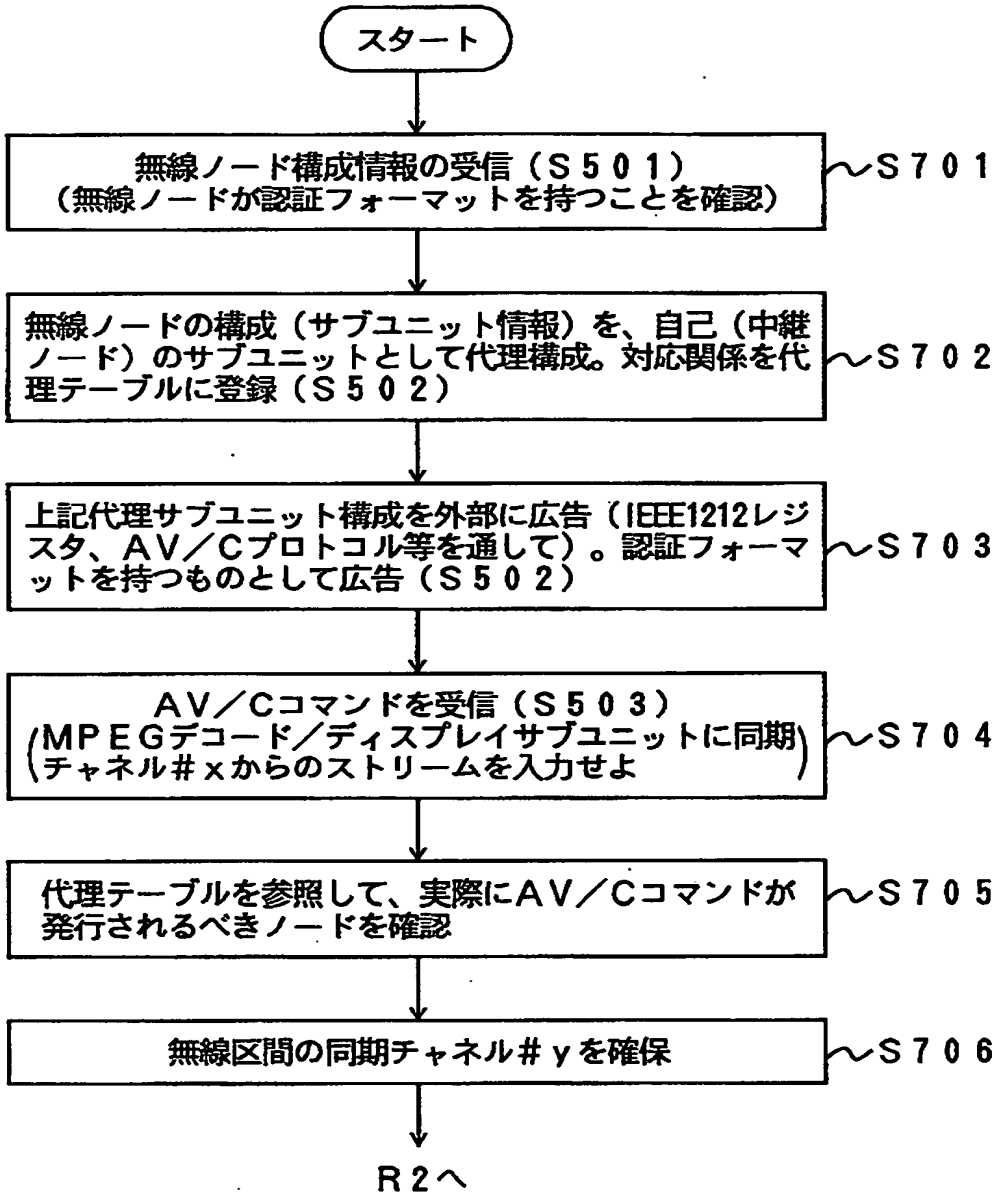
【図７】


スタート
中継ノード１０２内にＭＰＥＧデコード／ディスプレイサブユニットが存在すると認識（Ｓ５０２）
～Ｓ６０１
ＡＶ／Ｃプロトコルにて、１３９４バス上に同期チャネル＃ｘを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード１０２に送出(Ｓ５０３）
～Ｓ６０２
同期チャネル＃ｘを介して、暗号化されたＭＰＥＧ映像を送出（Ｓ５０６）
～Ｓ６０３
認識要求（Ｓ５０９）受信（中継ノードＭＰＥＧデコード／ディスプレイサブユニットからの受信と解釈）
～Ｓ６０４
Ｂの認証フォーマットＢｃｅｒｔを解き、Ｂｄｉｄ等を抽出
～Ｓ６０５
中継ノードのＭＰＥＧデコード／ディスプレイサブユニットに対して、自らの認証フォーマット（Ａｃｅｒｔ）等をＢｄｉｄと共に送出（Ｓ５１０）
～Ｓ６０６
パケット５１３を受信（中継ノードのＭＰＥＧデコード／ディスプレイサブユニットからの受信と解釈）
～Ｓ６０７
タンパの確認、Ｂｃｅｒｔの確認、認証鍵Ｋａｕｔｈの計算
～Ｓ６０８
Ｒ１へ

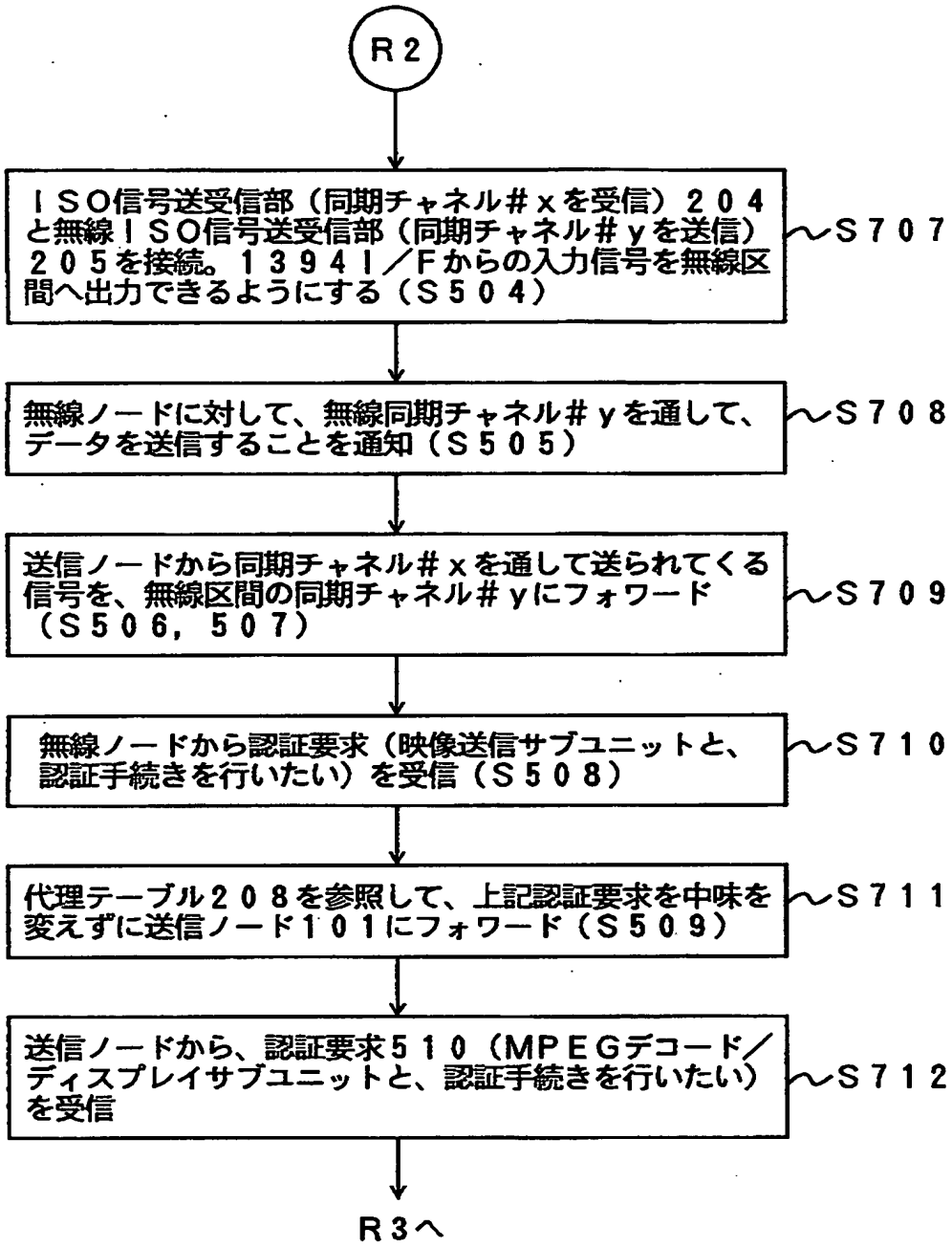
【図８】


R1
中継ノードのMPEGデコード／ディスプレイサブユニットに対して、認証・鍵交換手続き５１４の送信
S609
MPEG映像を鍵Kにて暗号化
S610
暗号化されたMPEG映像［MPEG映像］kを同期チャネル#xを通して送信（S518）
S611

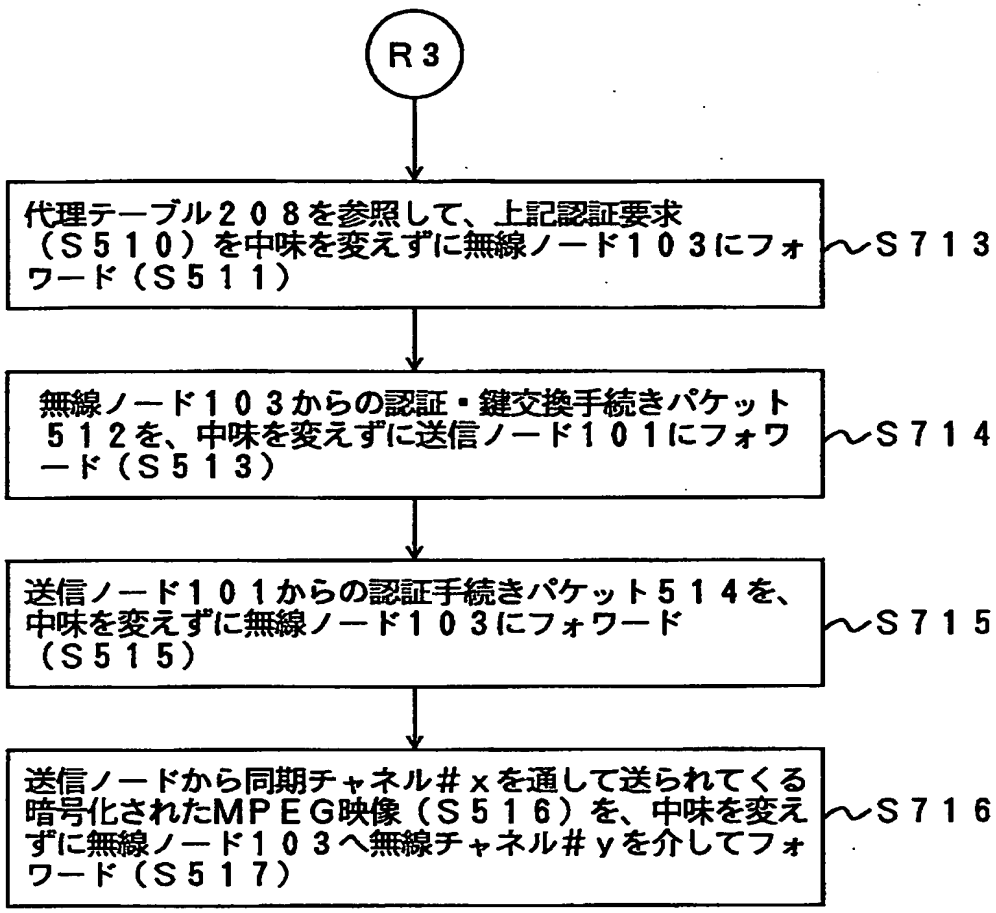
【図９】


スタート
無線ノード構成情報の受信（Ｓ５０１）
（無線ノードが認証フォーマットを持つことを確認）
Ｓ７０１
無線ノードの構成（サブユニット情報）を、自己（中継ノード）のサブユニットとして代理構成。対応関係を代理テーブルに登録（Ｓ５０２）
Ｓ７０２
上記代理サブユニット構成を外部に広告（IEEE1212レジスタ、ＡＶ／Ｃプロトコル等を通して）。認証フォーマットを持つものとして広告（Ｓ５０２）
Ｓ７０３
ＡＶ／Ｃコマンドを受信（Ｓ５０３）
（ＭＰＥＧデコード／ディスプレイサブユニットに同期
チャネル＃ｘからのストリームを入力せよ）
Ｓ７０４
代理テーブルを参照して、実際にＡＶ／Ｃコマンドが発行されるべきノードを確認
Ｓ７０５
無線区間の同期チャネル＃ｙを確保
Ｓ７０６
Ｒ２へ

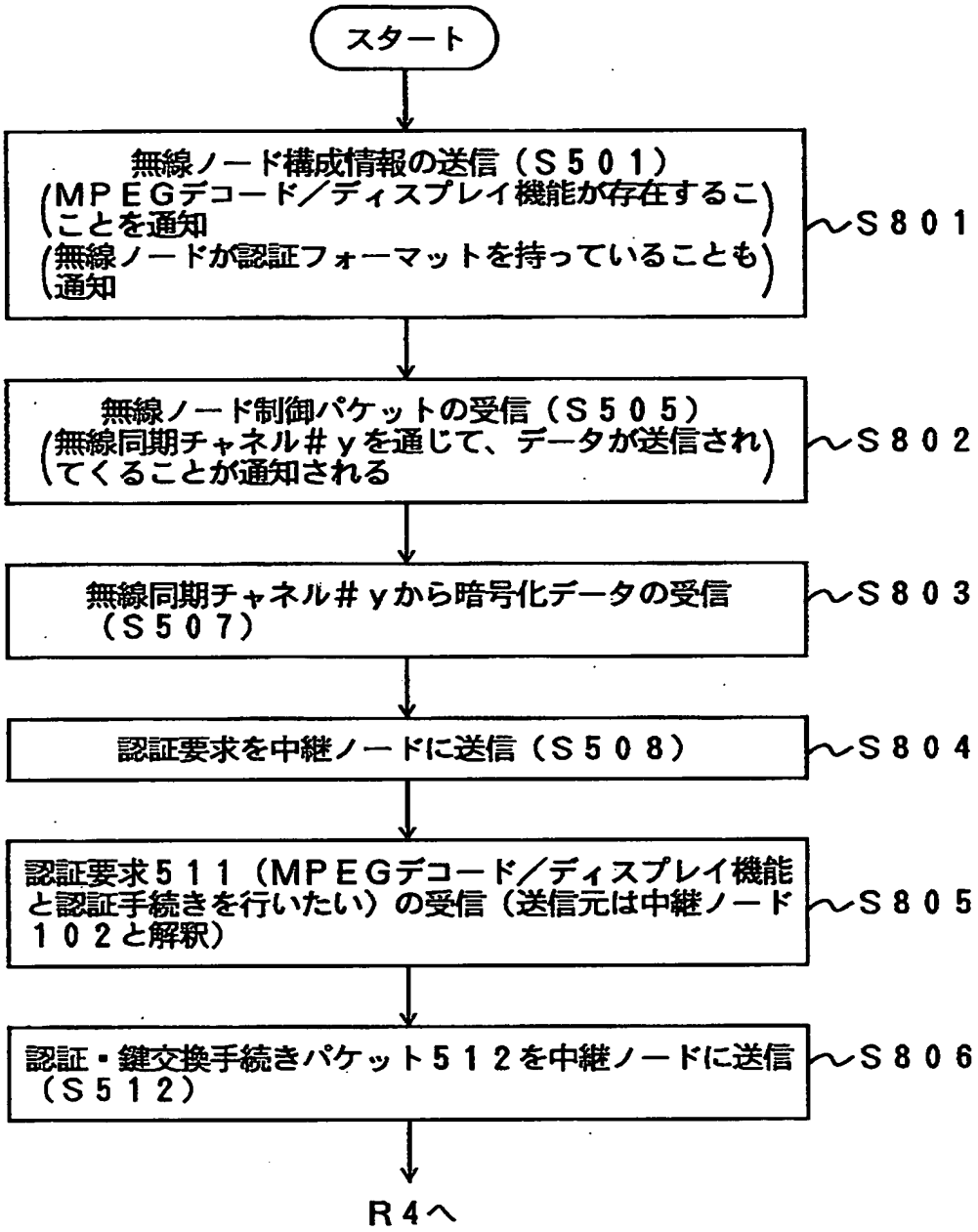
【図１０】


R2
ＩＳＯ信号送受信部（同期チャネル＃ｘを受信）２０４と無線ＩＳＯ信号送受信部（同期チャネル＃ｙを送信）２０５を接続。１３９４Ｉ／Ｆからの入力信号を無線区間へ出力できるようにする（Ｓ５０４）
Ｓ７０７
無線ノードに対して、無線同期チャネル＃ｙを通して、データを送信することを通知（Ｓ５０５）
Ｓ７０８
送信ノードから同期チャネル＃ｘを通して送られてくる信号を、無線区間の同期チャネル＃ｙにフォワード（Ｓ５０６，５０７）
Ｓ７０９
無線ノードから認証要求（映像送信サブユニットと、認証手続きを行いたい）を受信（Ｓ５０８）
Ｓ７１０
代理テーブル２０８を参照して、上記認証要求を中味を変えずに送信ノード１０１にフォワード（Ｓ５０９）
Ｓ７１１
送信ノードから、認証要求５１０（ＭＰＥＧデコード／ディスプレイサブユニットと、認証手続きを行いたい）を受信
Ｓ７１２
R3へ

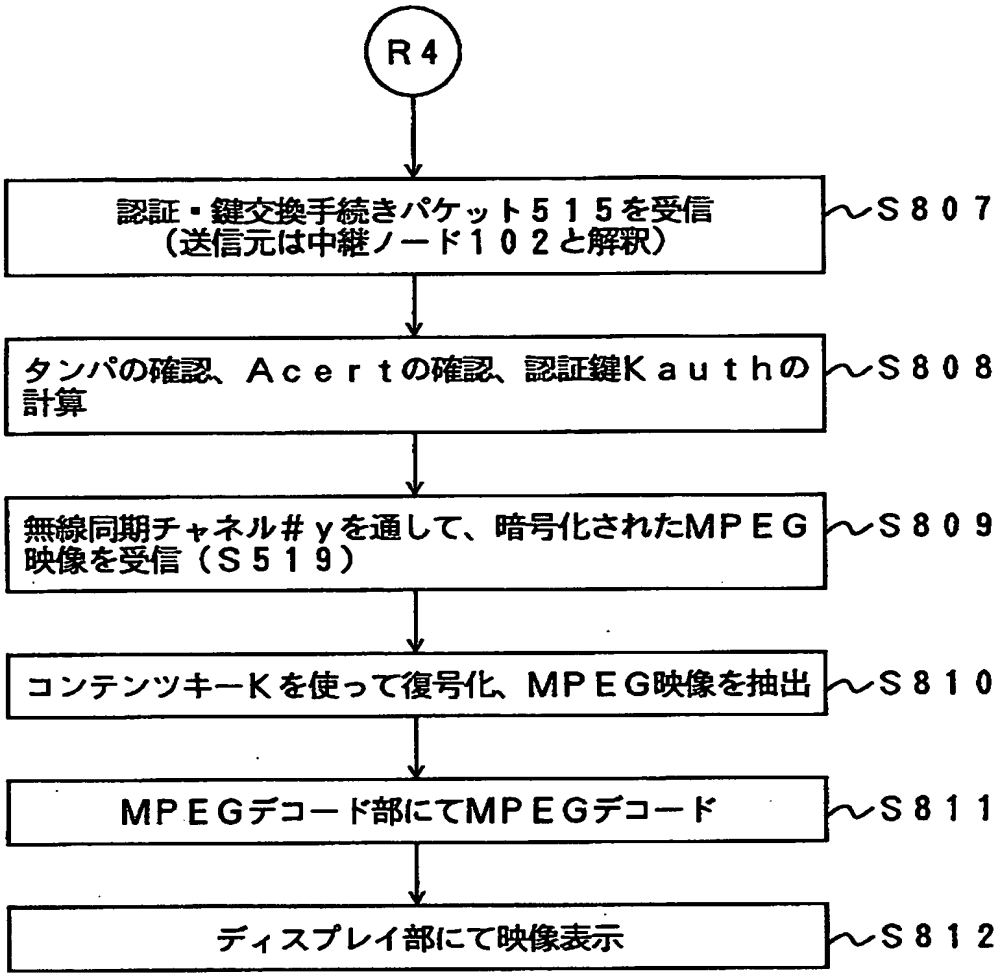
【図１１】


R3
代理テーブル２０８を参照して、上記認証要求（Ｓ５１０）を中味を変えずに無線ノード１０３にフォワード（Ｓ５１１）
～Ｓ７１３
無線ノード１０３からの認証・鍵交換手続きパケット５１２を、中味を変えずに送信ノード１０１にフォワード（Ｓ５１３）
～Ｓ７１４
送信ノード１０１からの認証手続きパケット５１４を、中味を変えずに無線ノード１０３にフォワード（Ｓ５１５）
～Ｓ７１５
送信ノードから同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像（Ｓ５１６）を、中味を変えずに無線ノード１０３へ無線チャネル＃ｙを介してフォワード（Ｓ５１７）
～Ｓ７１６

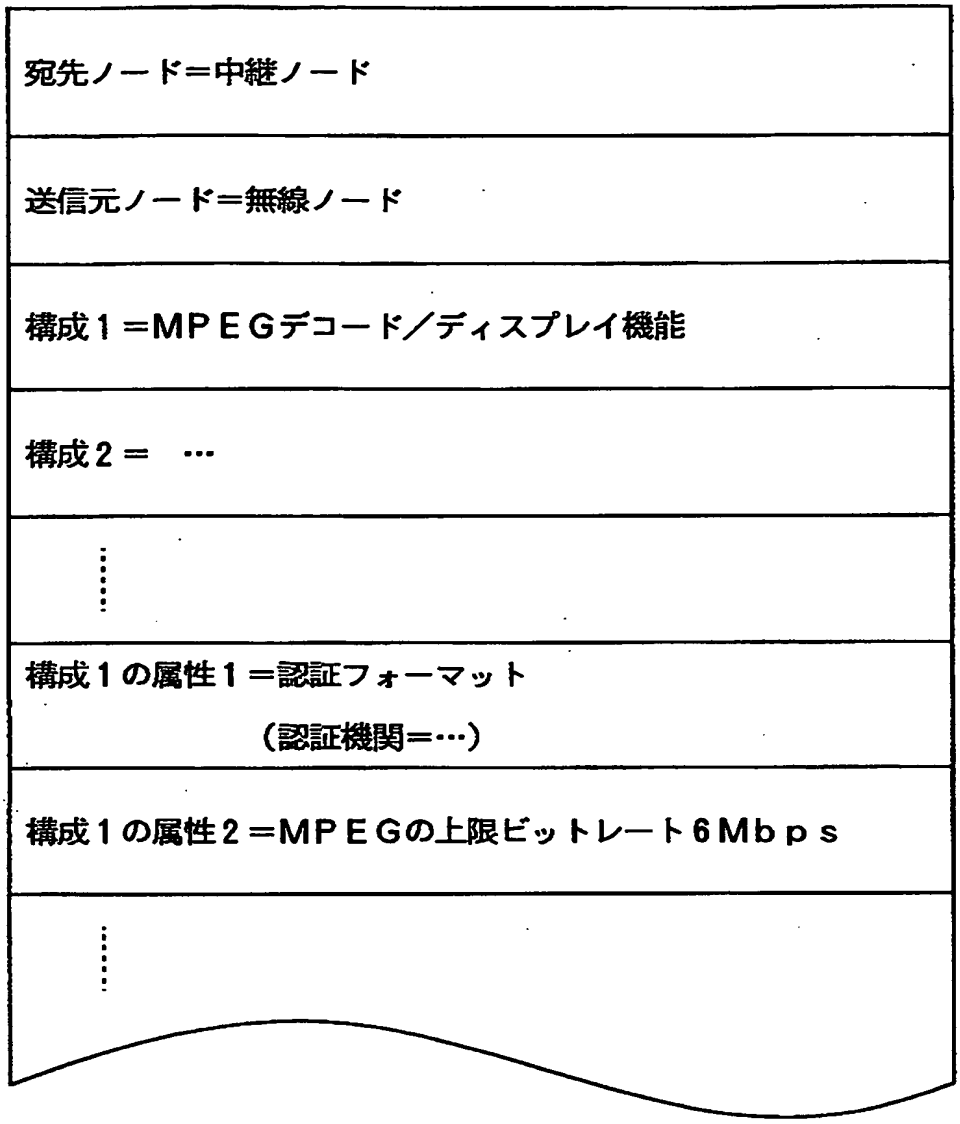
【図１２】


スタート
無線ノード構成情報の送信（Ｓ５０１）
(ＭＰＥＧデコード／ディスプレイ機能が存在することを通知
(無線ノードが認証フォーマットを持っていることも通知
～Ｓ８０１
無線ノード制御パケットの受信（Ｓ５０５）
(無線同期チャネル＃ｙを通じて、データが送信されてくることが通知される
～Ｓ８０２
無線同期チャネル＃ｙから暗号化データの受信（Ｓ５０７）
～Ｓ８０３
認証要求を中継ノードに送信（Ｓ５０８）
～Ｓ８０４
認証要求５１１（ＭＰＥＧデコード／ディスプレイ機能と認証手続きを行いたい）の受信（送信元は中継ノード１０２と解釈）
～Ｓ８０５
認証・鍵交換手続きパケット５１２を中継ノードに送信（Ｓ５１２）
～Ｓ８０６
Ｒ４へ

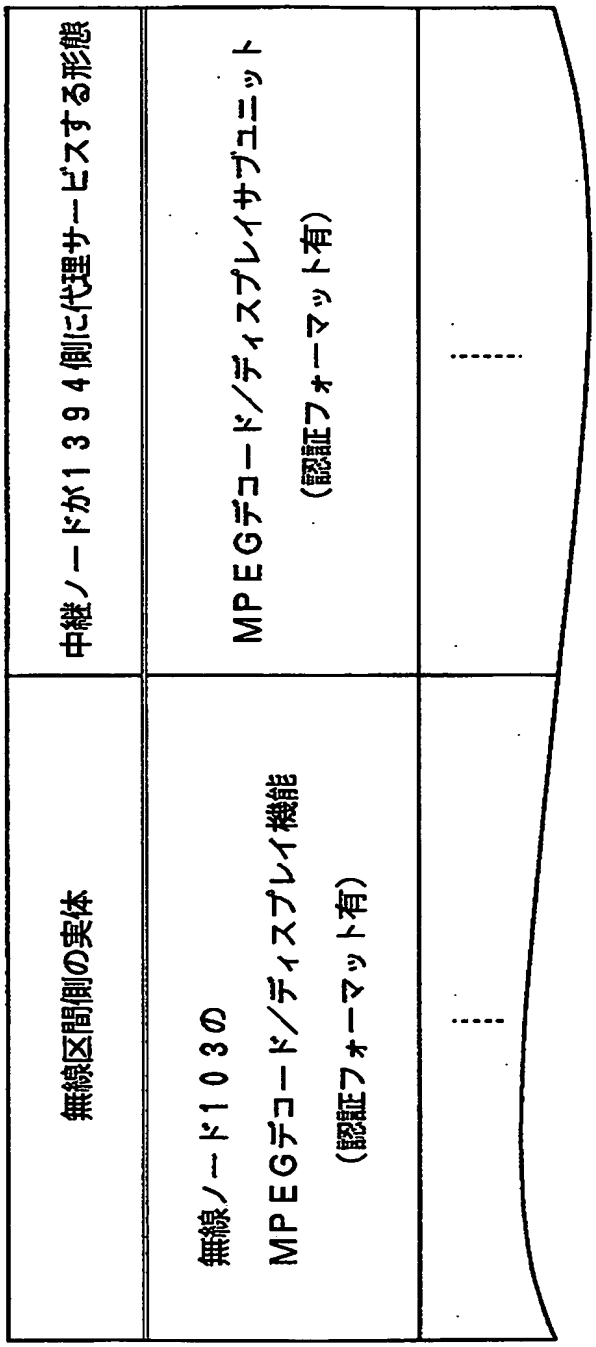
【図１３】


R4
認証・鍵交換手続きパケット５１５を受信
（送信元は中継ノード１０２と解釈）
～Ｓ８０７
タンパの確認、Ａｃｅｒｔの確認、認証鍵Ｋａｕｔｈの計算
～Ｓ８０８
無線同期チャネル＃ｙを通して、暗号化されたＭＰＥＧ映像を受信（Ｓ５１９）
～Ｓ８０９
コンテンツキーＫを使って復号化、ＭＰＥＧ映像を抽出
～Ｓ８１０
ＭＰＥＧデコード部にてＭＰＥＧデコード
～Ｓ８１１
ディスプレイ部にて映像表示
～Ｓ８１２

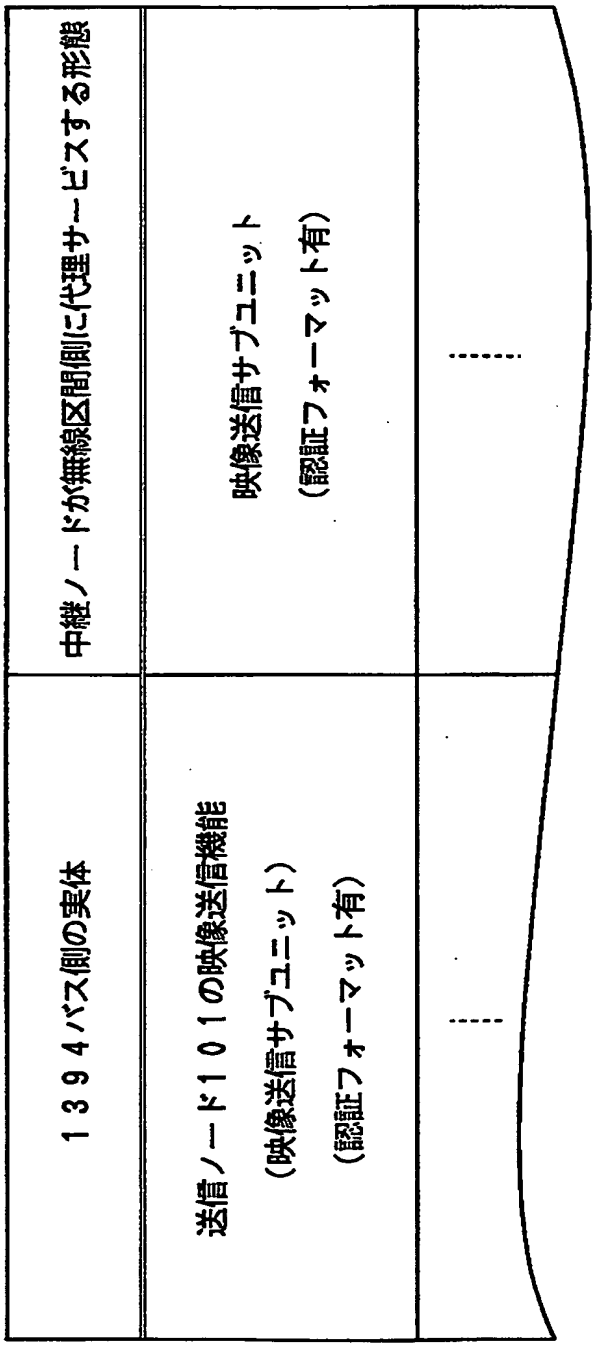
【図１４】


宛先ノード＝中継ノード
送信元ノード＝無線ノード
構成１＝ＭＰＥＧデコード／ディスプレイ機能
構成２＝　…
構成１の属性１＝認証フォーマット
（認証機関＝…）
構成１の属性２＝ＭＰＥＧの上限ビットレート６Ｍｂｐｓ

【図１５】

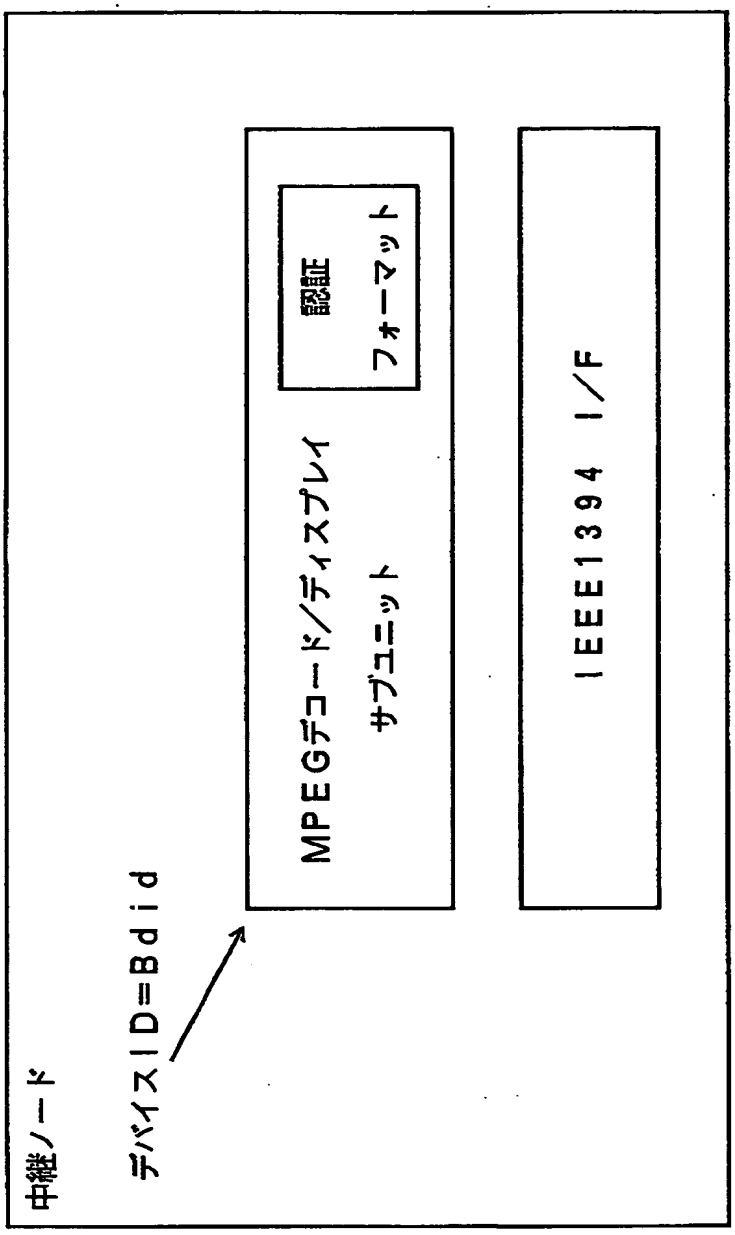

無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の
MPEGデコード／ディスプレイ機能
（認証フォーマット有）
MPEGデコード／ディスプレイサブユニット
（認証フォーマット有）

【図１６】

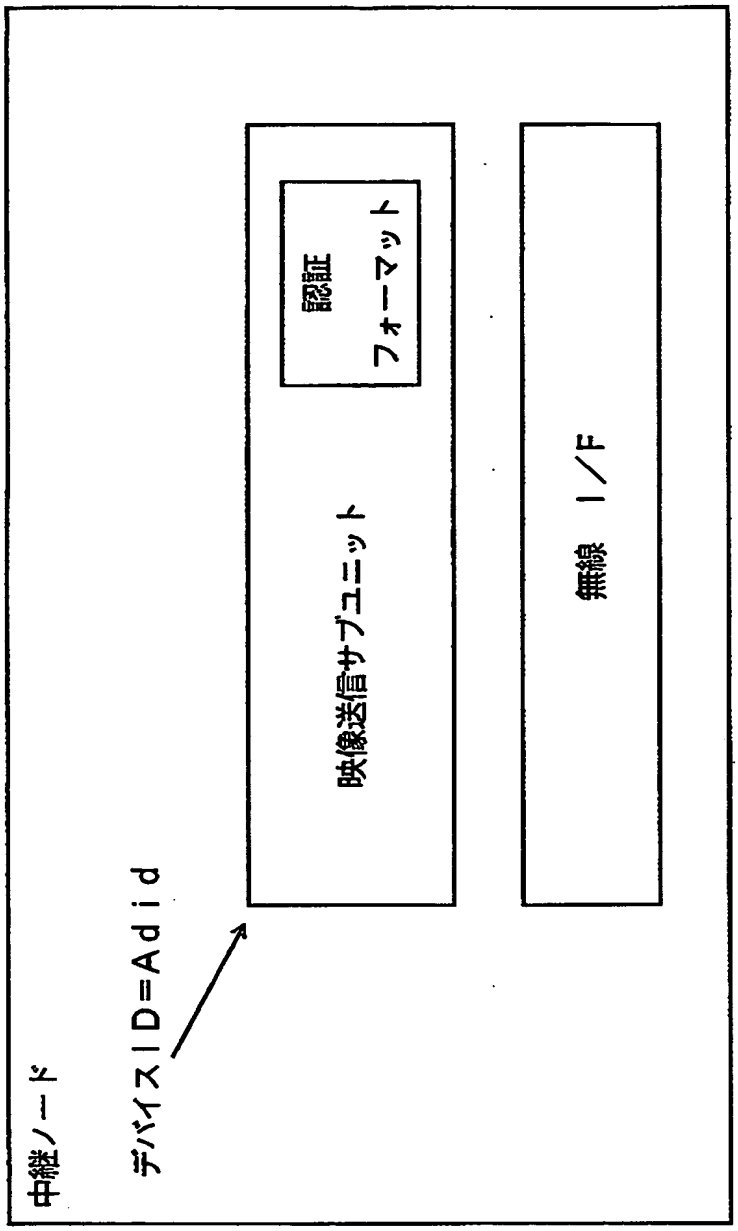

中継ノードが無線区間側に代理サービスする形態
映像送信サブユニット
（認証フォーマット有）

１３９４バス側の実体
送信ノード１０１の映像送信機能
（映像送信サブユニット）
（認証フォーマット有）

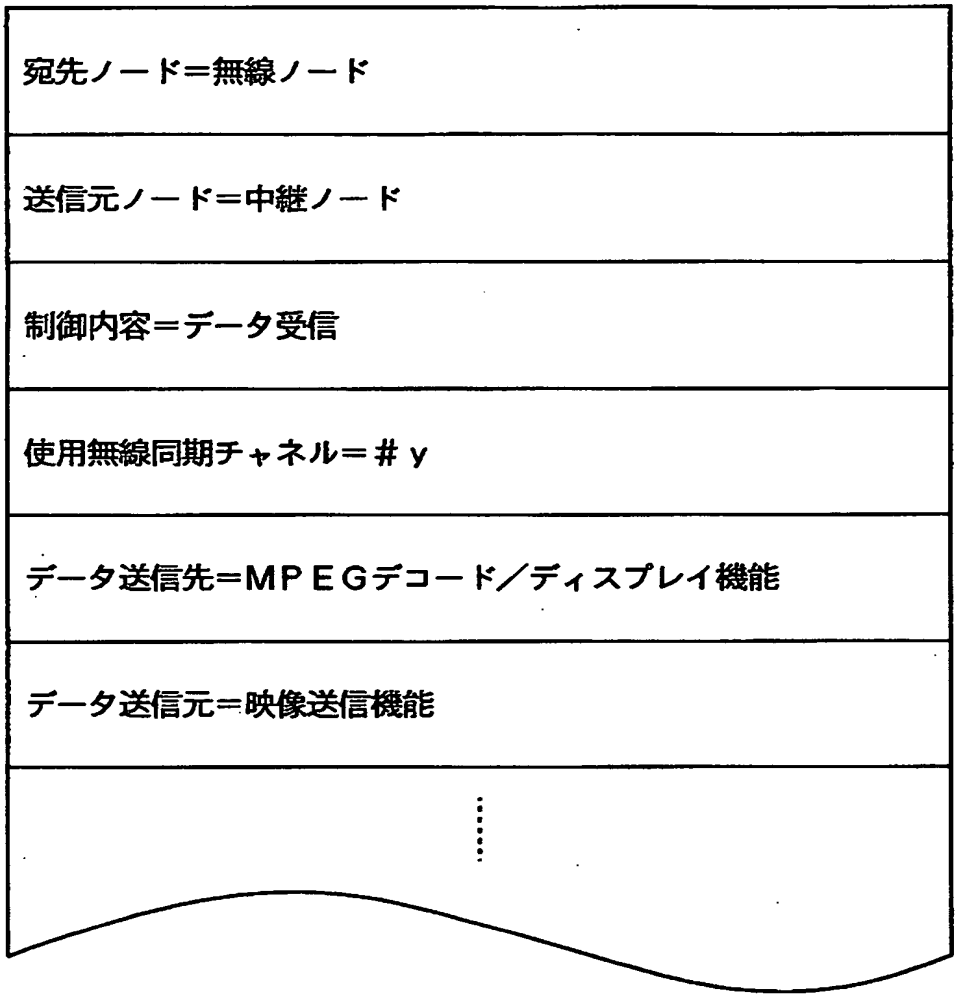
【図１７】


中継ノード
デバイスＩＤ=Ｂｄｉｄ
ＭＰＥＧデコード／ディスプレイ
サブユニット
認証
フォーマット
ＩＥＥＥ１３９４　Ｉ／Ｆ

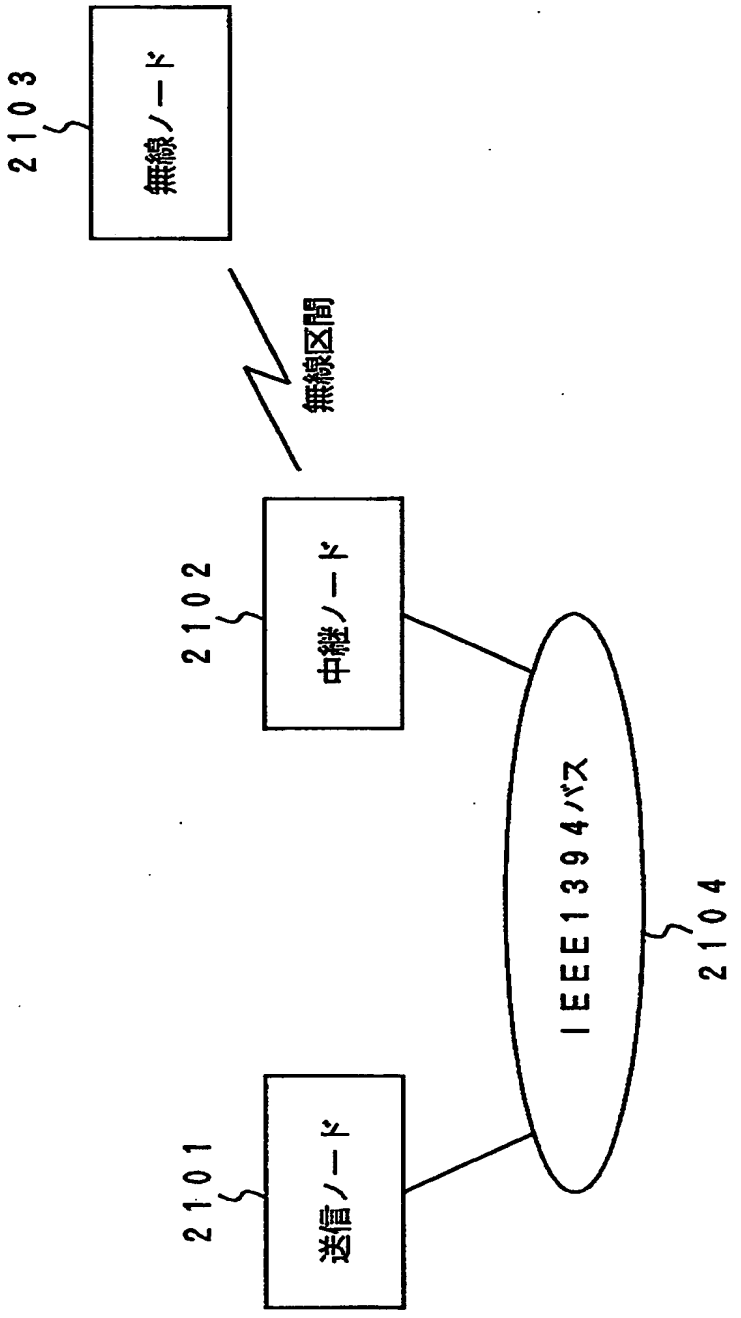
【図１８】



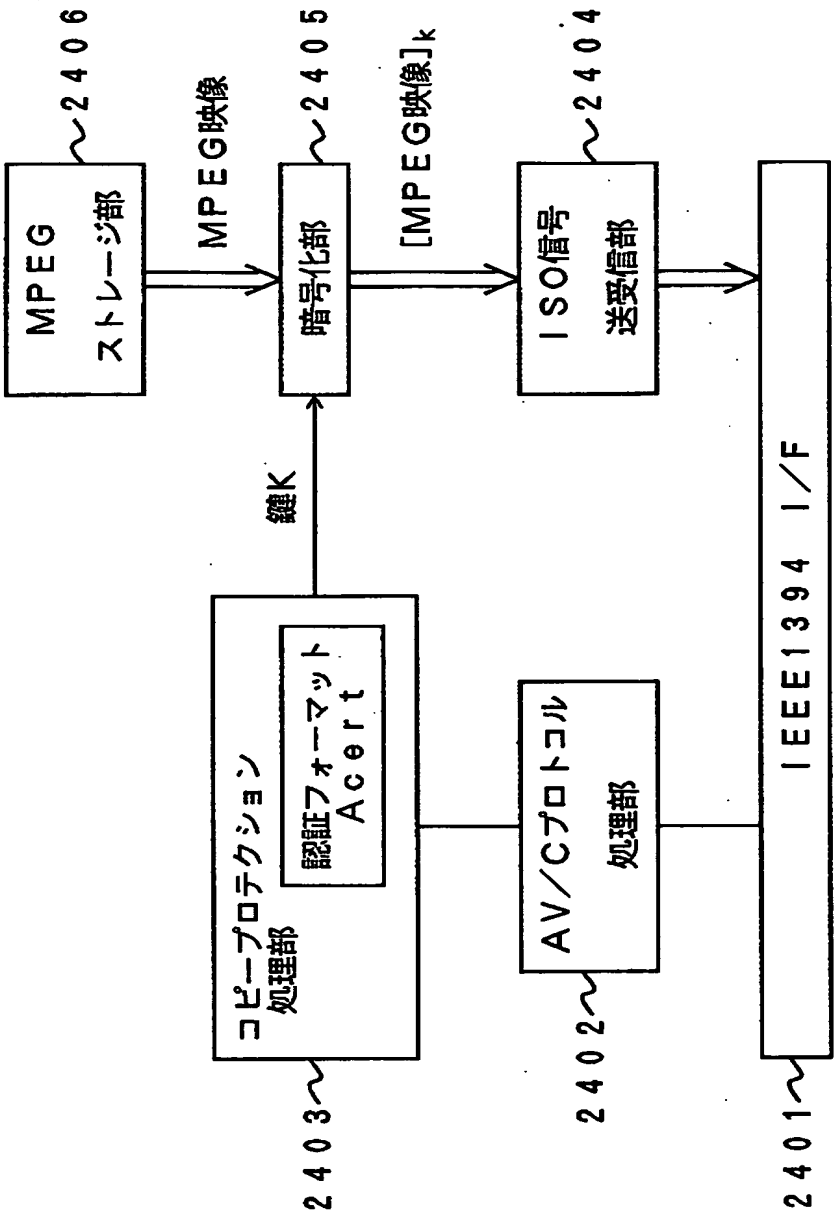
【図１９】


宛先ノード＝無線ノード
送信元ノード＝中継ノード
制御内容＝データ受信
使用無線同期チャネル＝＃ｙ
データ送信先＝ＭＰＥＧデコード／ディスプレイ機能
データ送信元＝映像送信機能

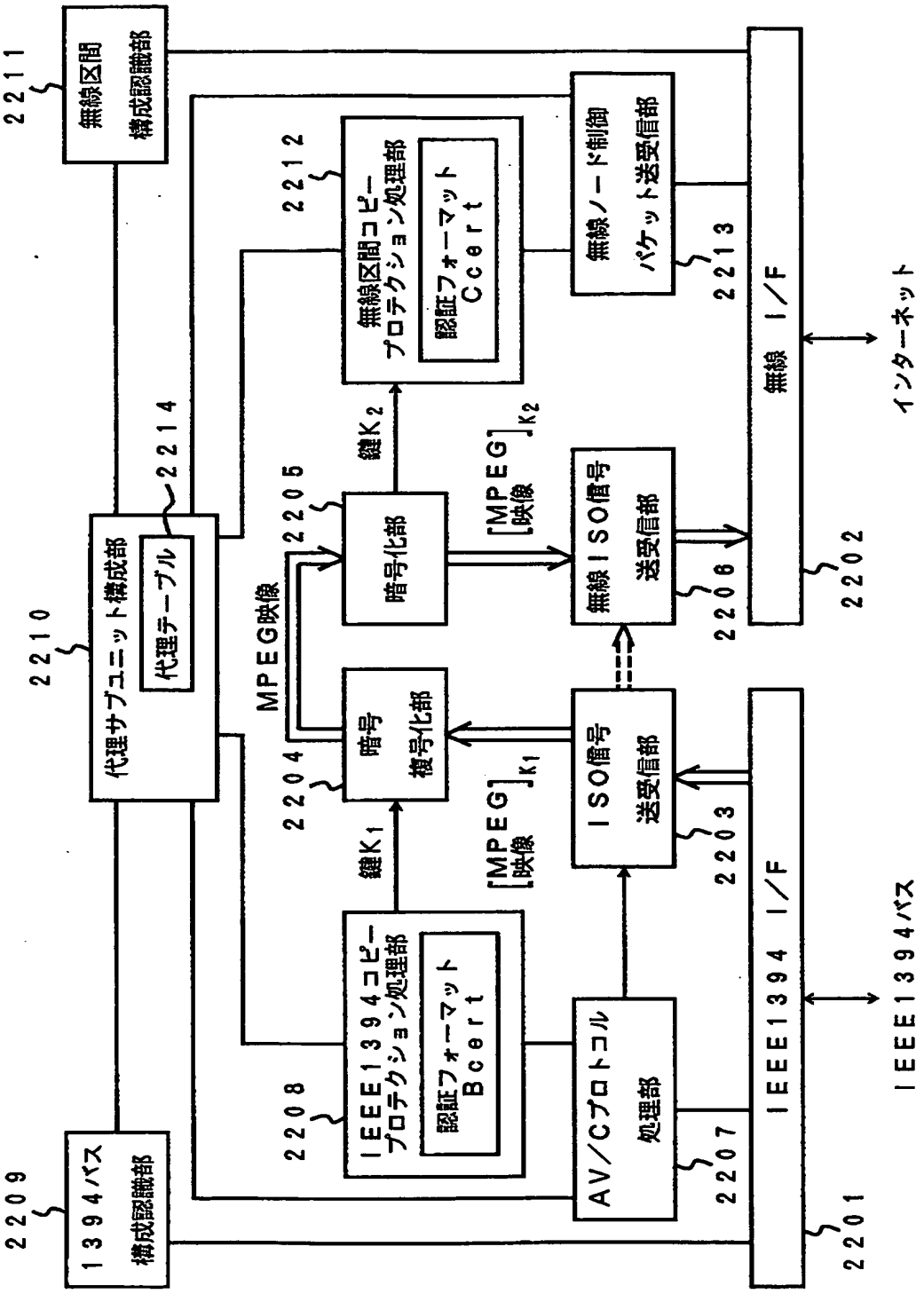
【図２０】



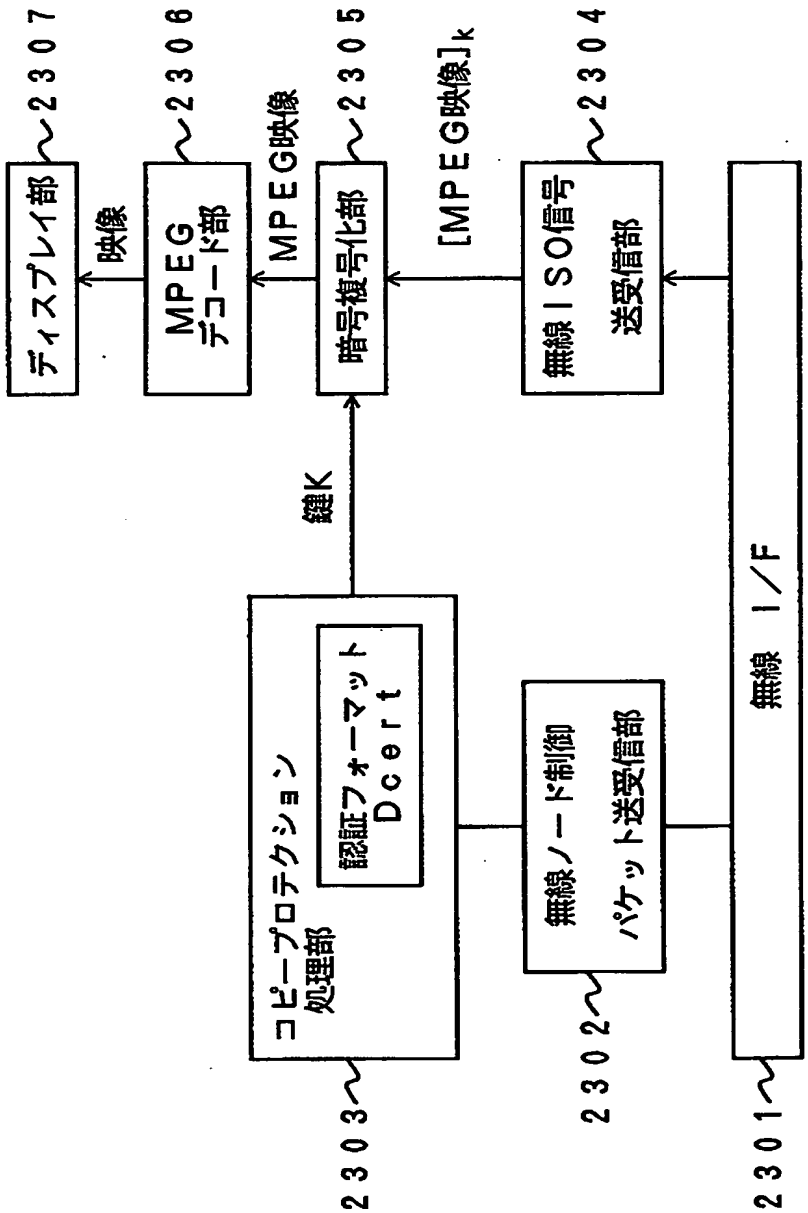
【図２１】


MPEG
ストレージ部
2406
MPEG映像
暗号化部
2405
[MPEG映像]k
ISO信号
送受信部
2404
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
2403
AV/Cプロトコル
処理部
2402
IEEE1394 I/F
2401

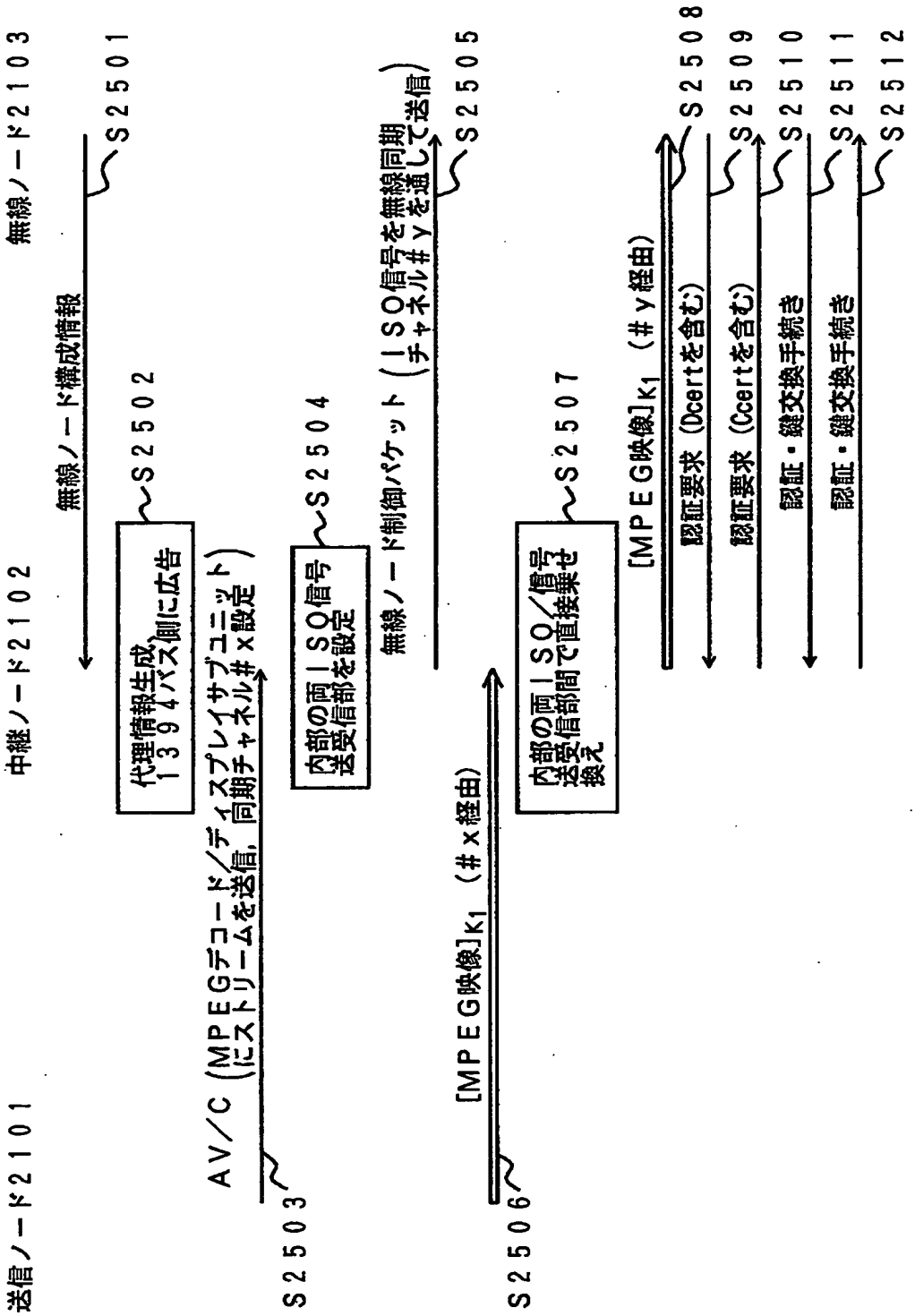
【図２２】


無線区間
構成認識部
2211
無線区間コピー
プロテクション処理部
認証フォーマット
Ccert
2212
無線ノード制御
パケット送受信部
2213
無線 I／F
インターネット
2202
代理サブユニット構成部
代理テーブル
2214
2210
鍵K2
2205
暗号化部
[MPEG
映像]K2
無線ISO信号
送受信部
2206
MPEG映像
暗号
複号化部
2204
鍵K1
[MPEG
映像]K1
ISO信号
送受信部
2203
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
2208
AV／Cプロトコル
処理部
2207
IEEE1394 I／F
IEEE1394バス
2201
1394バス
構成認識部
2209

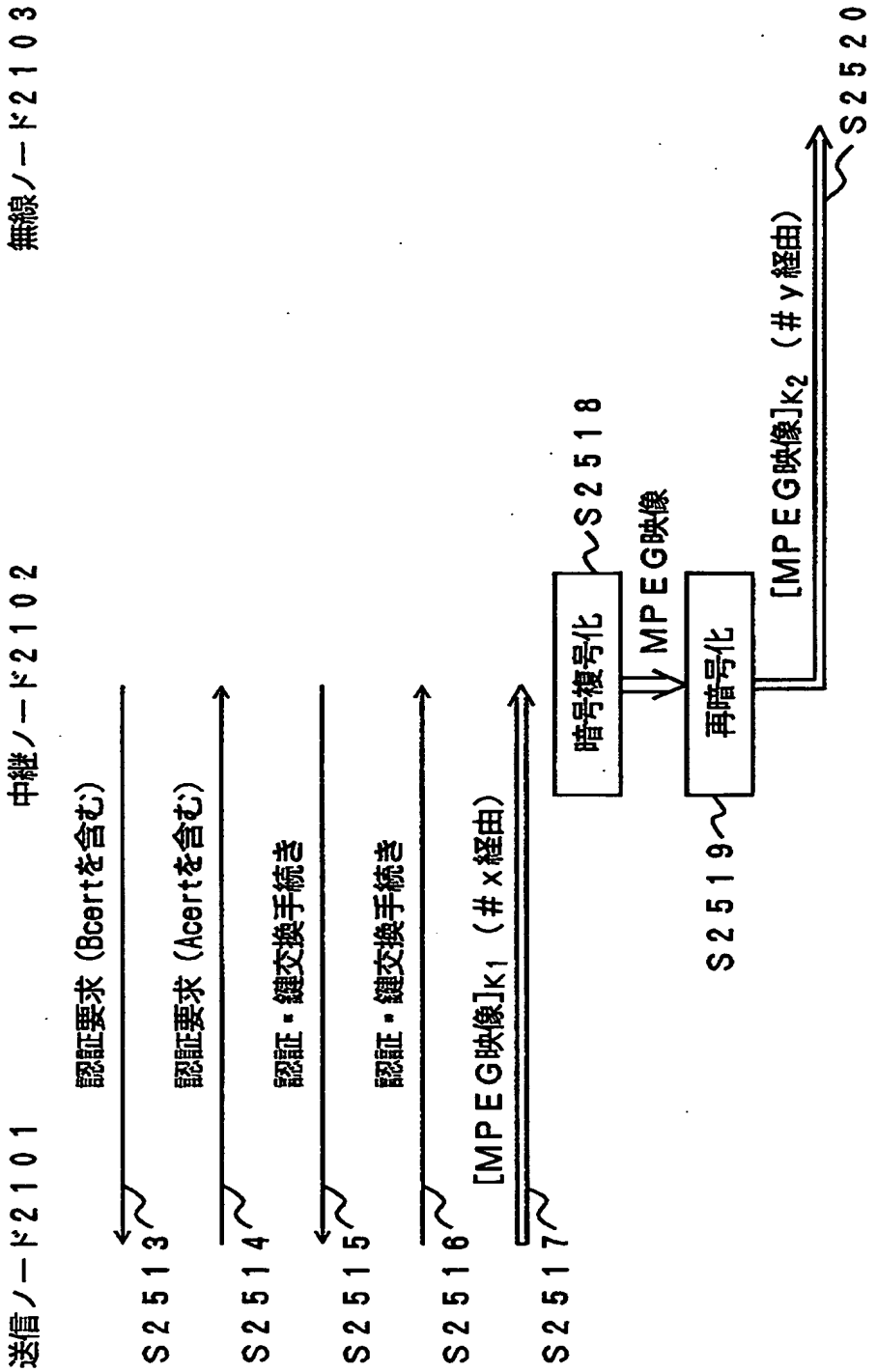
【図２３】


ディスプレイ部
2307
映像
MPEG
デコード部
2306
MPEG映像
暗号複号化部
2305
[MPEG映像]k
無線ISO信号
送受信部
2304
鍵K
コピープロテクション
処理部
認証フォーマット
Dcert
2303
無線ノード制御
パケット送受信部
2302
無線 I/F
2301

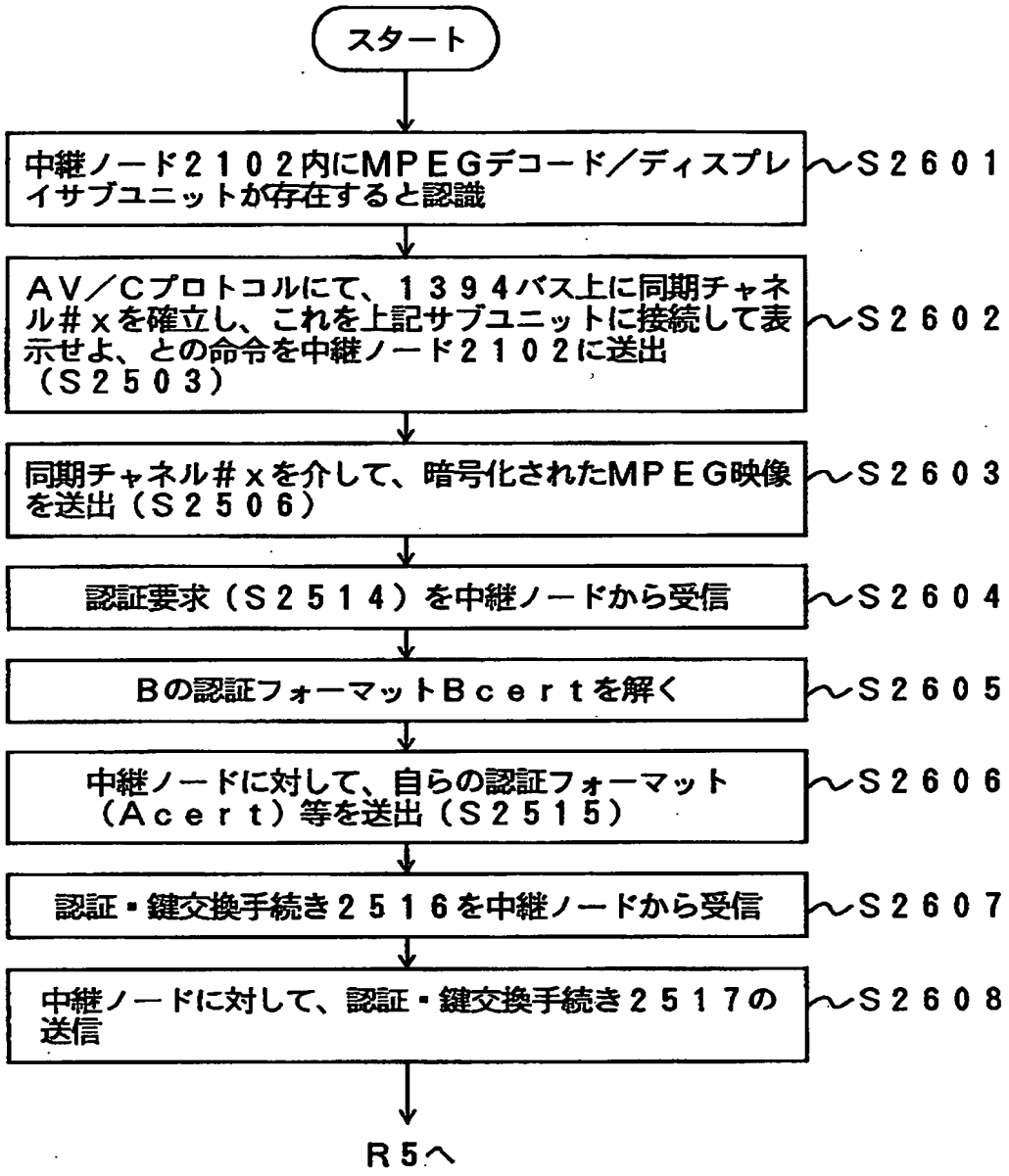
【図２４】


送信ノード2101
中継ノード2102
無線ノード2103
無線ノード構成情報
S2501
代理情報生成
1394バス側に広告
S2502
AV/C (MPEGデコード/ディスプレイサブユニット)
(にストリームを送信, 同期チャネル#x設定)
S2503
内部の両ISO信号
送受信部を設定
S2504
無線ノード制御パケット (ISO信号を無線同期
チャネル#yを通して送信)
S2505
[MPEG映像]K1 (#x経由)
S2506
内部の両ISO信号
送受信部間で直接乗せ
換え
S2507
[MPEG映像]K1 (#y経由)
認証要求 (Dcertを含む)
S2508
認証要求 (Ccertを含む)
S2509
認証・鍵交換手続き
S2510
認証・鍵交換手続き
S2511
S2512

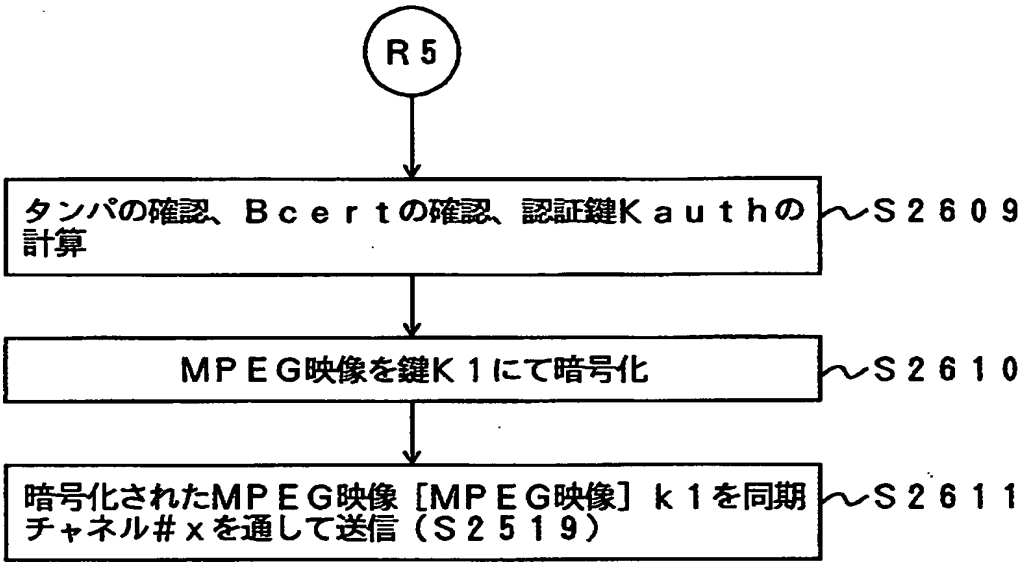
【図２５】


送信ノード2101
中継ノード2102
無線ノード2103
認証要求 (Bcertを含む)
S2513
認証要求 (Acertを含む)
S2514
認証・鍵交換手続き
S2515
認証・鍵交換手続き
S2516
[MPEG映像]K1 (#x経由)
S2517
暗号複号化
S2518
MPEG映像
再暗号化
S2519
[MPEG映像]K2 (#y経由)
S2520

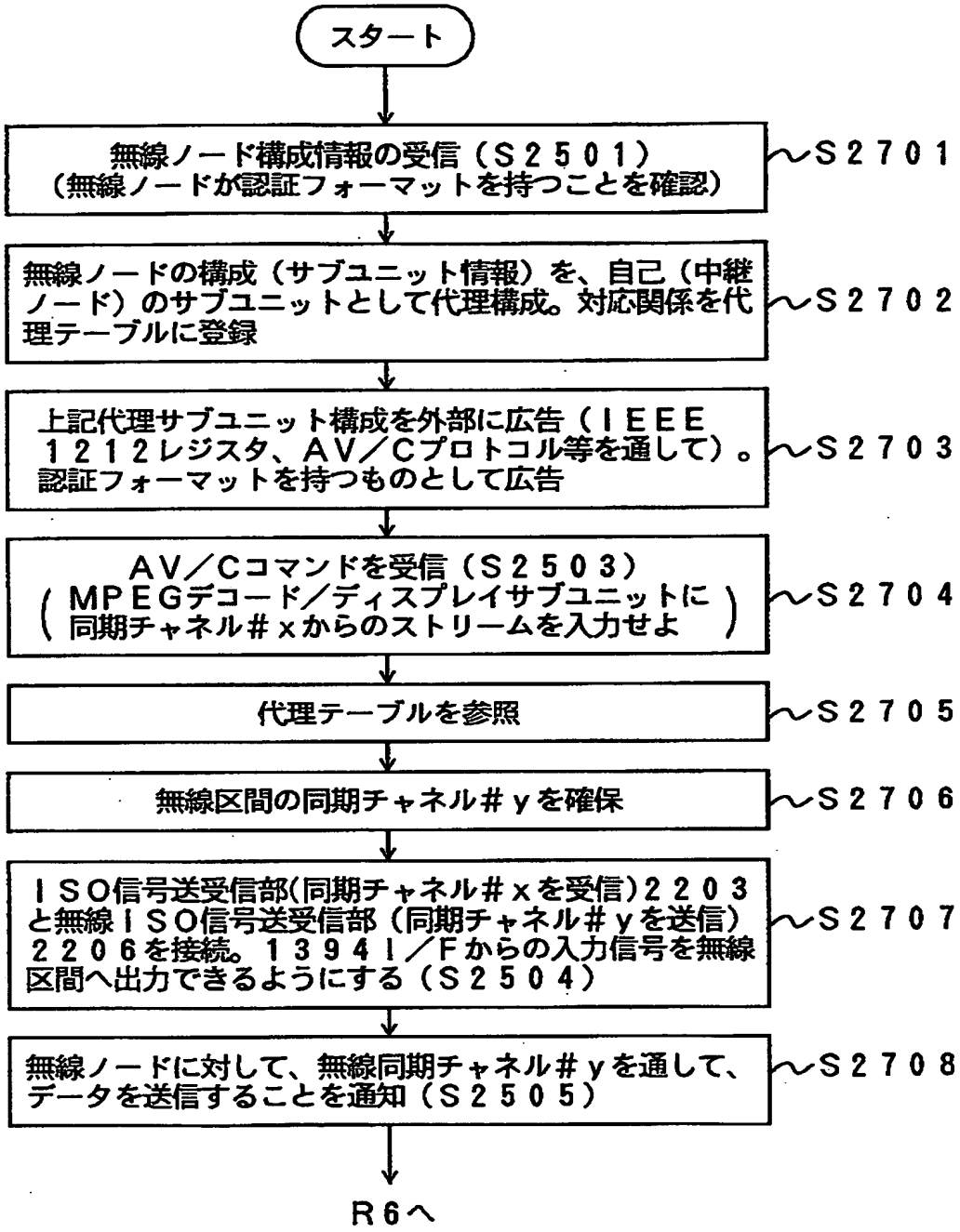
【図２６】


スタート
中継ノード２１０２内にＭＰＥＧデコード／ディスプレイサブユニットが存在すると認識
～Ｓ２６０１
ＡＶ／Ｃプロトコルにて、１３９４バス上に同期チャネル＃ｘを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード２１０２に送出（Ｓ２５０３）
～Ｓ２６０２
同期チャネル＃ｘを介して、暗号化されたＭＰＥＧ映像を送出（Ｓ２５０６）
～Ｓ２６０３
認証要求（Ｓ２５１４）を中継ノードから受信
～Ｓ２６０４
Ｂの認証フォーマットＢｃｅｒｔを解く
～Ｓ２６０５
中継ノードに対して、自らの認証フォーマット（Ａｃｅｒｔ）等を送出（Ｓ２５１５）
～Ｓ２６０６
認証・鍵交換手続き２５１６を中継ノードから受信
～Ｓ２６０７
中継ノードに対して、認証・鍵交換手続き２５１７の送信
～Ｓ２６０８
Ｒ５へ

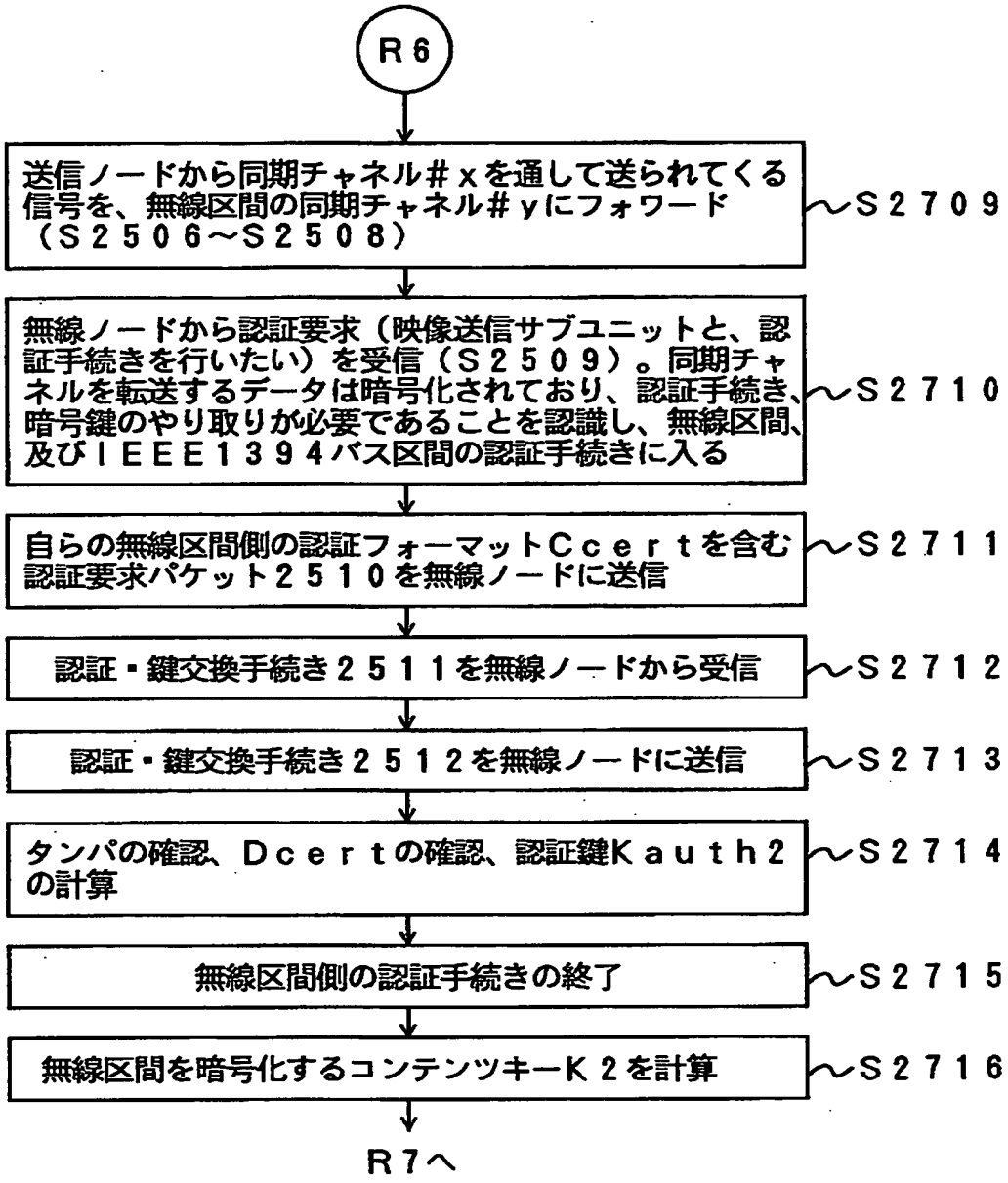
【図２７】


R5
タンパの確認、Ｂｃｅｒｔの確認、認証鍵Ｋａｕｔｈの計算
Ｓ２６０９
ＭＰＥＧ映像を鍵Ｋ１にて暗号化
Ｓ２６１０
暗号化されたＭＰＥＧ映像［ＭＰＥＧ映像］ｋ１を同期チャネル＃ｘを通して送信（Ｓ２５１９）
Ｓ２６１１

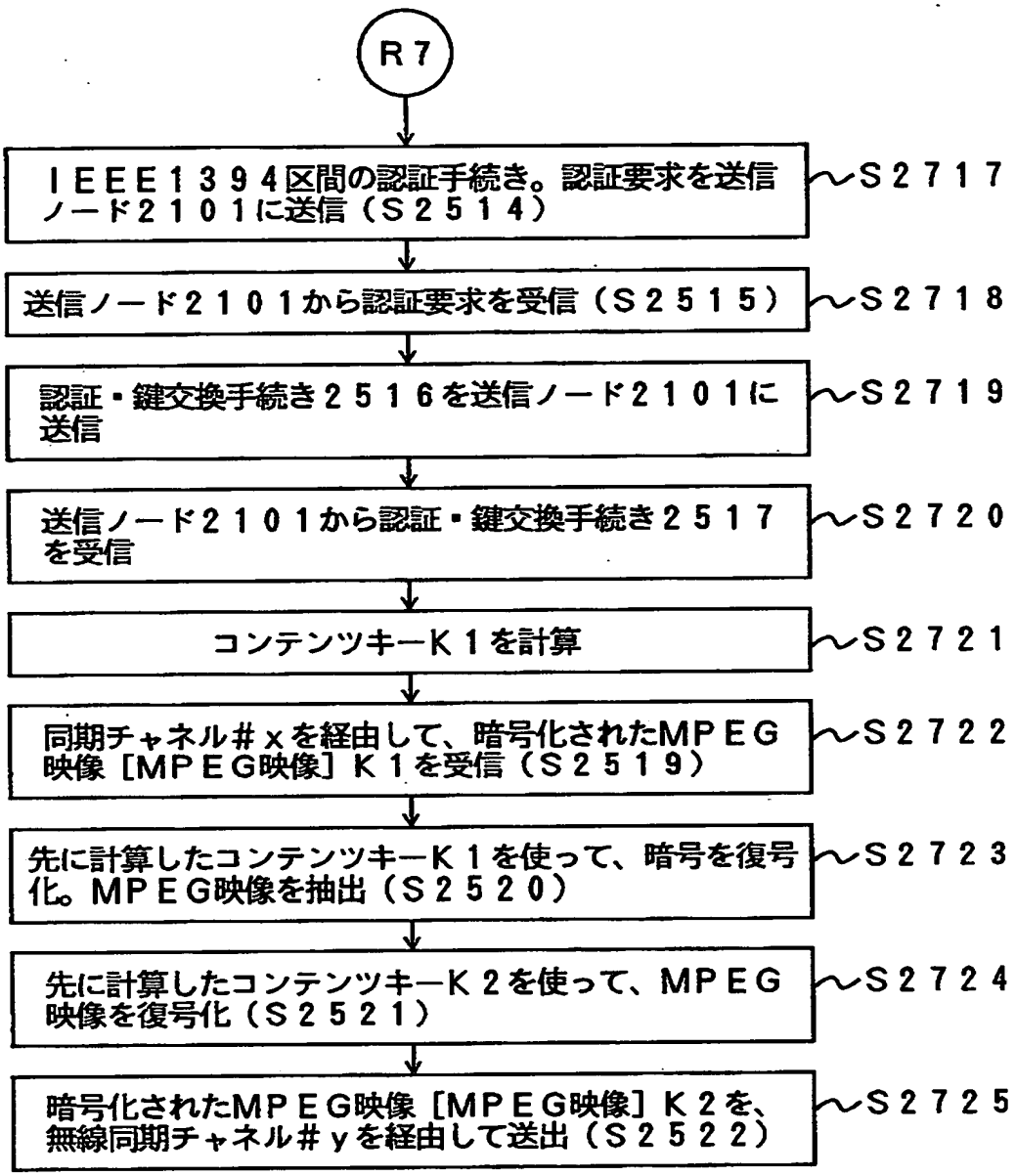
【図２８】


スタート
無線ノード構成情報の受信（Ｓ２５０１）
（無線ノードが認証フォーマットを持つことを確認）
Ｓ２７０１
無線ノードの構成（サブユニット情報）を、自己（中継ノード）のサブユニットとして代理構成。対応関係を代理テーブルに登録
Ｓ２７０２
上記代理サブユニット構成を外部に広告（ＩＥＥＥ１２１２レジスタ、ＡＶ／Ｃプロトコル等を通して）。認証フォーマットを持つものとして広告
Ｓ２７０３
ＡＶ／Ｃコマンドを受信（Ｓ２５０３）
（ＭＰＥＧデコード／ディスプレイサブユニットに同期チャネル＃ｘからのストリームを入力せよ）
Ｓ２７０４
代理テーブルを参照
Ｓ２７０５
無線区間の同期チャネル＃ｙを確保
Ｓ２７０６
ＩＳＯ信号送受信部(同期チャネル＃ｘを受信)２２０３と無線ＩＳＯ信号送受信部（同期チャネル＃ｙを送信）２２０６を接続。１３９４Ｉ／Ｆからの入力信号を無線区間へ出力できるようにする（Ｓ２５０４）
Ｓ２７０７
無線ノードに対して、無線同期チャネル＃ｙを通して、データを送信することを通知（Ｓ２５０５）
Ｓ２７０８
Ｒ６へ

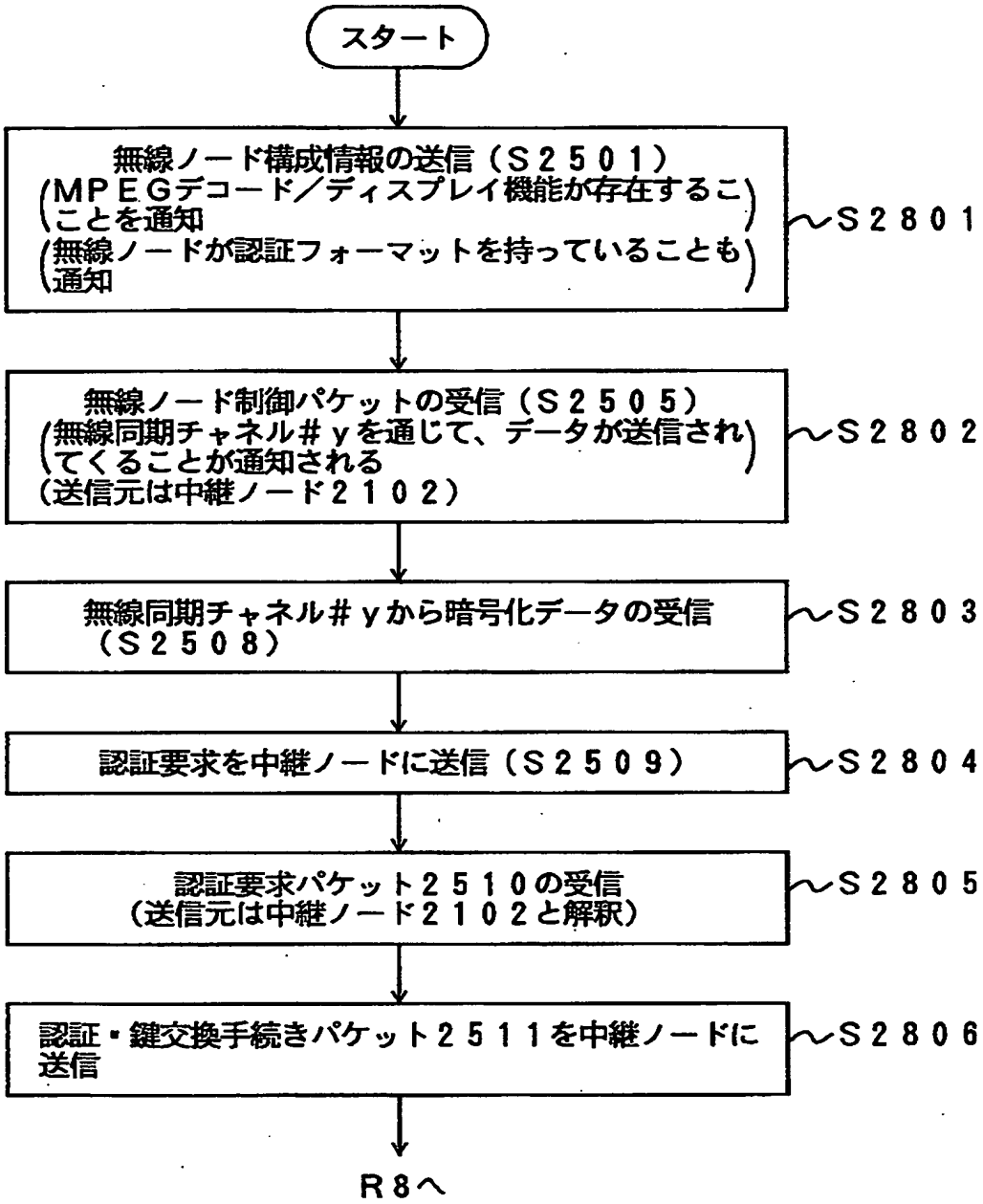
【図２９】


R6
送信ノードから同期チャネル＃ｘを通して送られてくる信号を、無線区間の同期チャネル＃ｙにフォワード（Ｓ２５０６～Ｓ２５０８）
～Ｓ２７０９
無線ノードから認証要求（映像送信サブユニットと、認証手続きを行いたい）を受信（Ｓ２５０９）。同期チャネルを転送するデータは暗号化されており、認証手続き、暗号鍵のやり取りが必要であることを認識し、無線区間、及びＩＥＥＥ１３９４バス区間の認証手続きに入る
～Ｓ２７１０
自らの無線区間側の認証フォーマットＣｃｅｒｔを含む認証要求パケット２５１０を無線ノードに送信
～Ｓ２７１１
認証・鍵交換手続き２５１１を無線ノードから受信
～Ｓ２７１２
認証・鍵交換手続き２５１２を無線ノードに送信
～Ｓ２７１３
タンパの確認、Ｄｃｅｒｔの確認、認証鍵Ｋａｕｔｈ２の計算
～Ｓ２７１４
無線区間側の認証手続きの終了
～Ｓ２７１５
無線区間を暗号化するコンテンツキーＫ２を計算
～Ｓ２７１６
R7へ

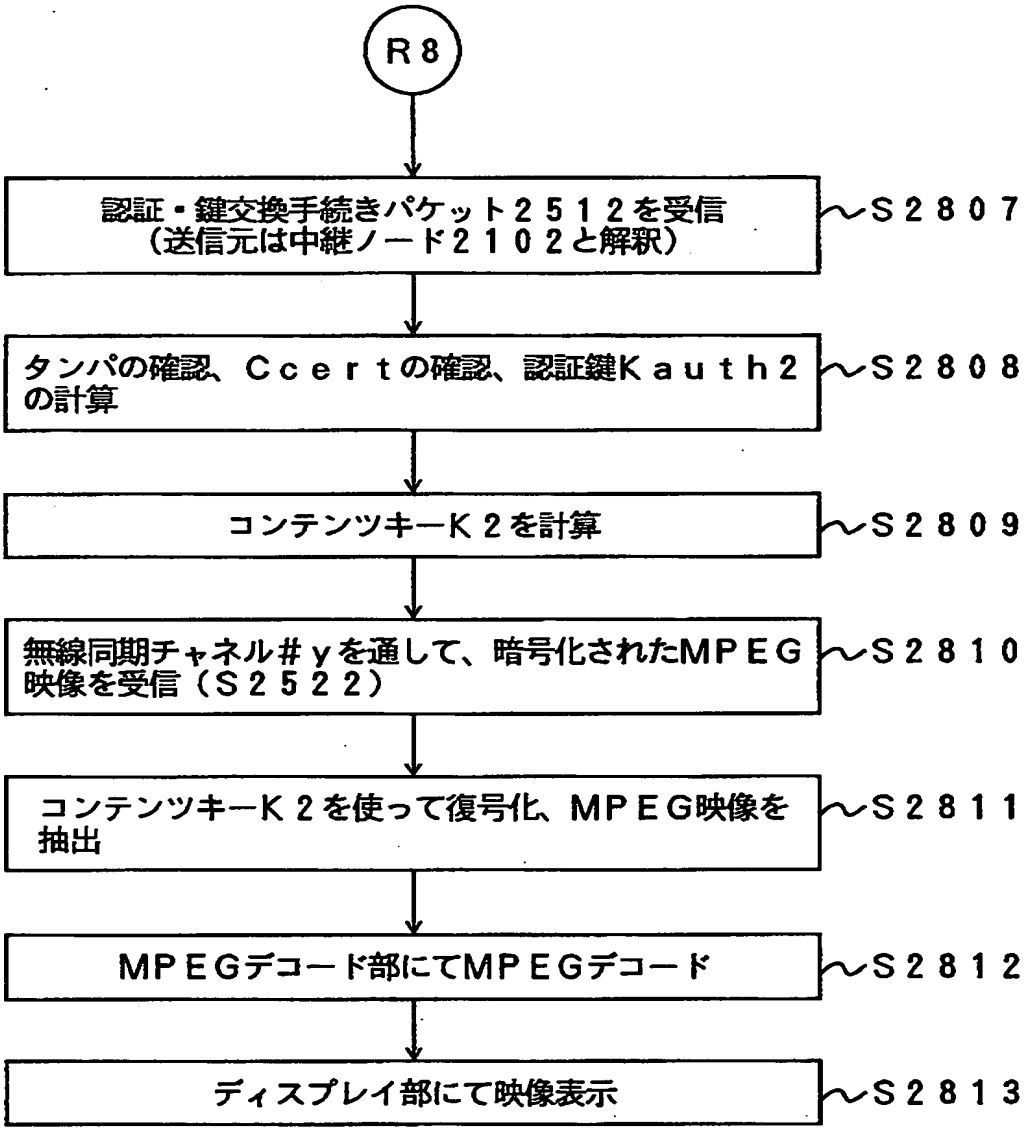
【図３０】


R7
ＩＥＥＥ１３９４区間の認証手続き。認証要求を送信ノード２１０１に送信（Ｓ２５１４）
Ｓ２７１７
送信ノード２１０１から認証要求を受信（Ｓ２５１５）
Ｓ２７１８
認証・鍵交換手続き２５１６を送信ノード２１０１に送信
Ｓ２７１９
送信ノード２１０１から認証・鍵交換手続き２５１７を受信
Ｓ２７２０
コンテンツキーＫ１を計算
Ｓ２７２１
同期チャネル＃ｘを経由して、暗号化されたＭＰＥＧ映像［ＭＰＥＧ映像］Ｋ１を受信（Ｓ２５１９）
Ｓ２７２２
先に計算したコンテンツキーＫ１を使って、暗号を復号化。ＭＰＥＧ映像を抽出（Ｓ２５２０）
Ｓ２７２３
先に計算したコンテンツキーＫ２を使って、ＭＰＥＧ映像を復号化（Ｓ２５２１）
Ｓ２７２４
暗号化されたＭＰＥＧ映像［ＭＰＥＧ映像］Ｋ２を、無線同期チャネル＃ｙを経由して送出（Ｓ２５２２）
Ｓ２７２５

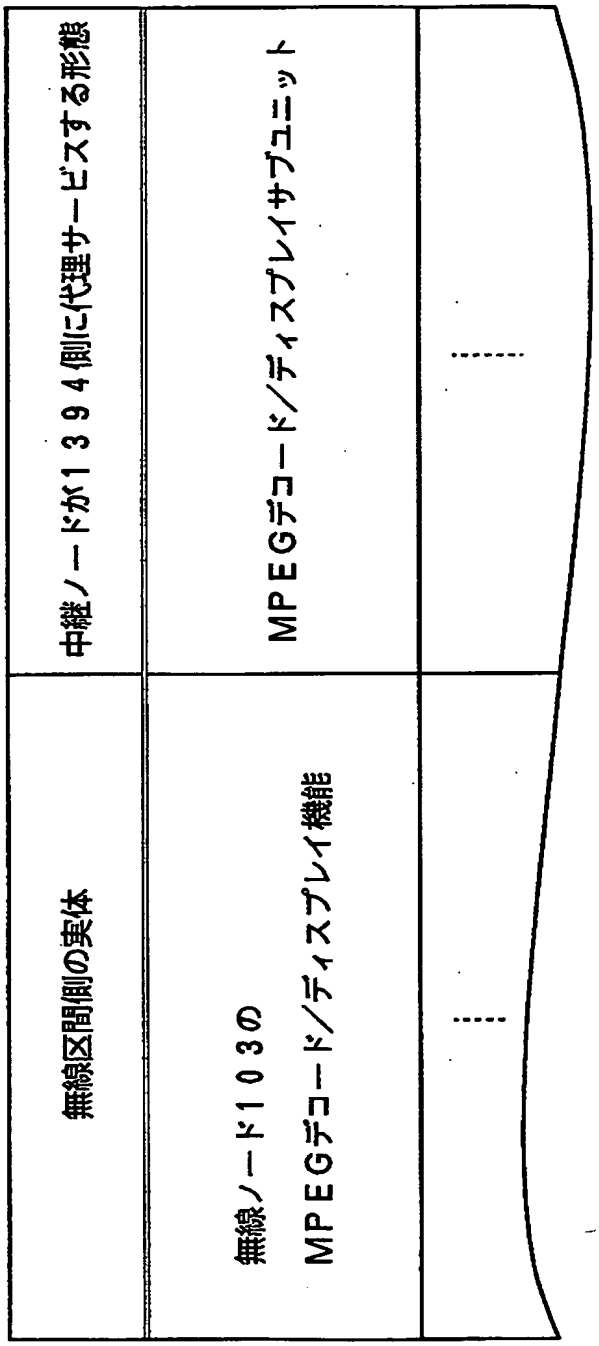
【図３１】


スタート
無線ノード構成情報の送信（Ｓ２５０１）
(ＭＰＥＧデコード／ディスプレイ機能が存在することを通知
(無線ノードが認証フォーマットを持っていることも通知
～Ｓ２８０１
無線ノード制御パケットの受信（Ｓ２５０５）
(無線同期チャネル＃ｙを通じて、データが送信されてくることが通知される
(送信元は中継ノード２１０２）
～Ｓ２８０２
無線同期チャネル＃ｙから暗号化データの受信（Ｓ２５０８）
～Ｓ２８０３
認証要求を中継ノードに送信（Ｓ２５０９）
～Ｓ２８０４
認証要求パケット２５１０の受信
（送信元は中継ノード２１０２と解釈）
～Ｓ２８０５
認証・鍵交換手続きパケット２５１１を中継ノードに送信
～Ｓ２８０６
Ｒ８へ

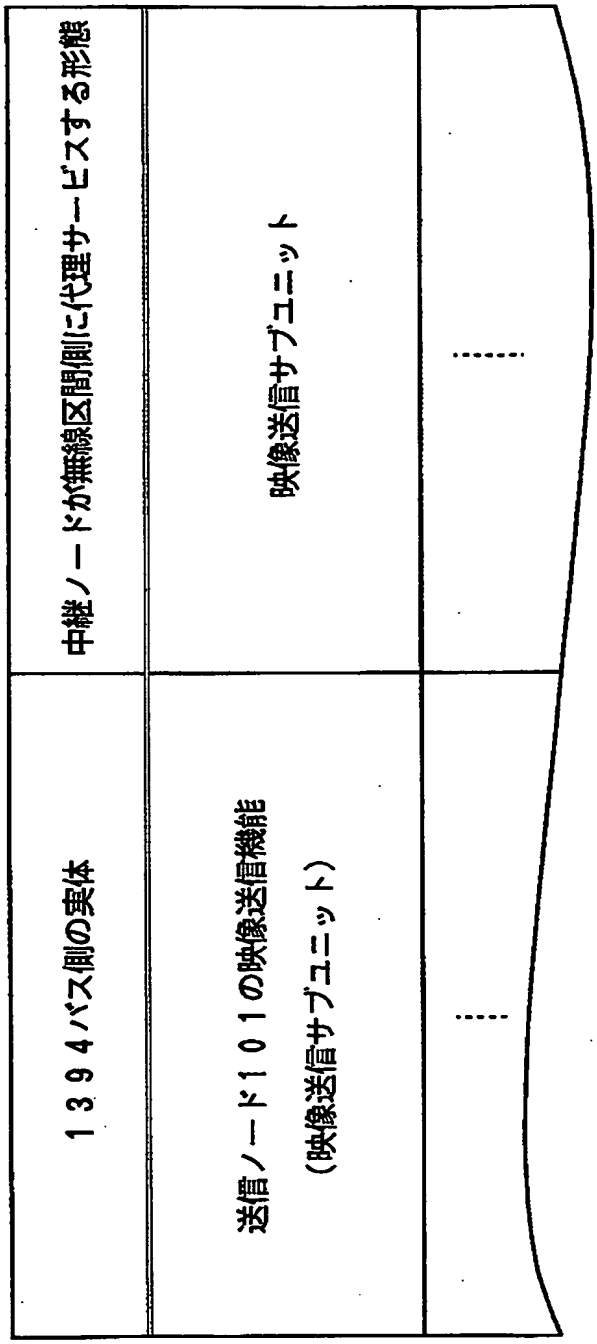
【図３２】


R8
認証・鍵交換手続きパケット２５１２を受信
（送信元は中継ノード２１０２と解釈）
～Ｓ２８０７
タンパの確認、Ｃｃｅｒｔの確認、認証鍵Ｋａｕｔｈ２の計算
～Ｓ２８０８
コンテンツキーＫ２を計算
～Ｓ２８０９
無線同期チャネル＃ｙを通して、暗号化されたＭＰＥＧ映像を受信（Ｓ２５２２）
～Ｓ２８１０
コンテンツキーＫ２を使って復号化、ＭＰＥＧ映像を抽出
～Ｓ２８１１
ＭＰＥＧデコード部にてＭＰＥＧデコード
～Ｓ２８１２
ディスプレイ部にて映像表示
～Ｓ２８１３

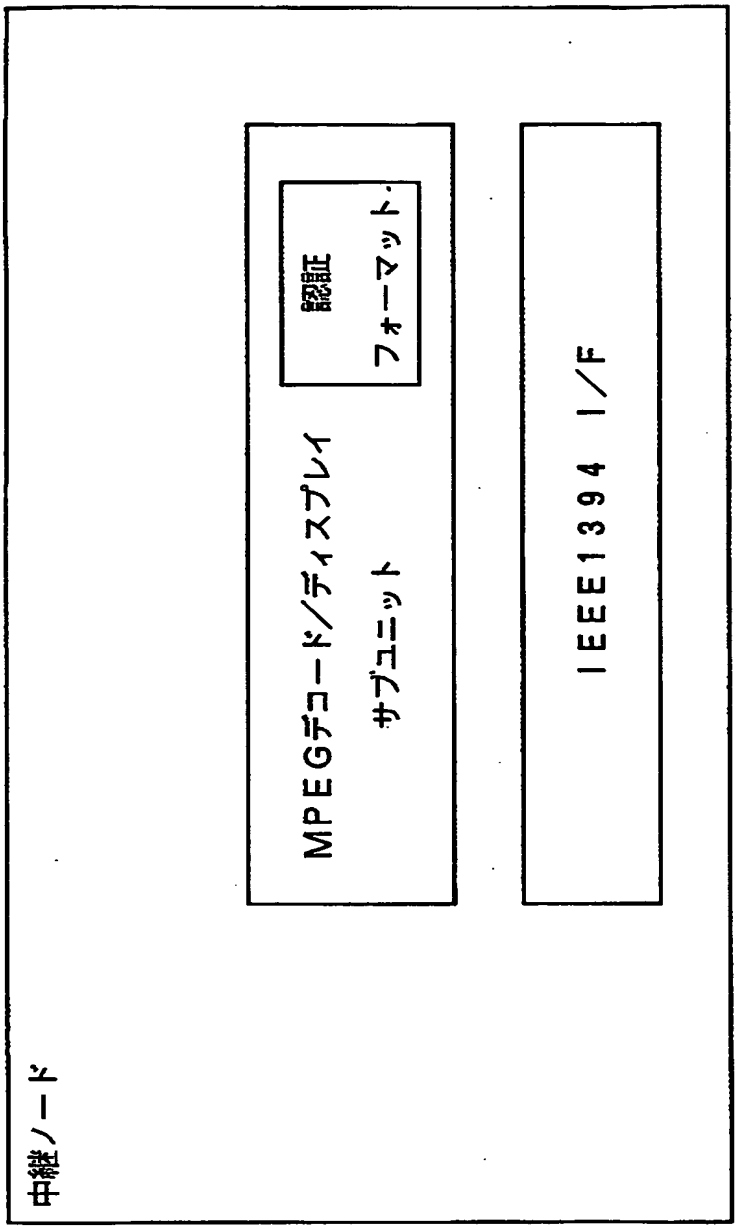
【図３３】


無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の
MPEGデコード／ディスプレイ機能
MPEGデコード／ディスプレイサブユニット

【図３４】

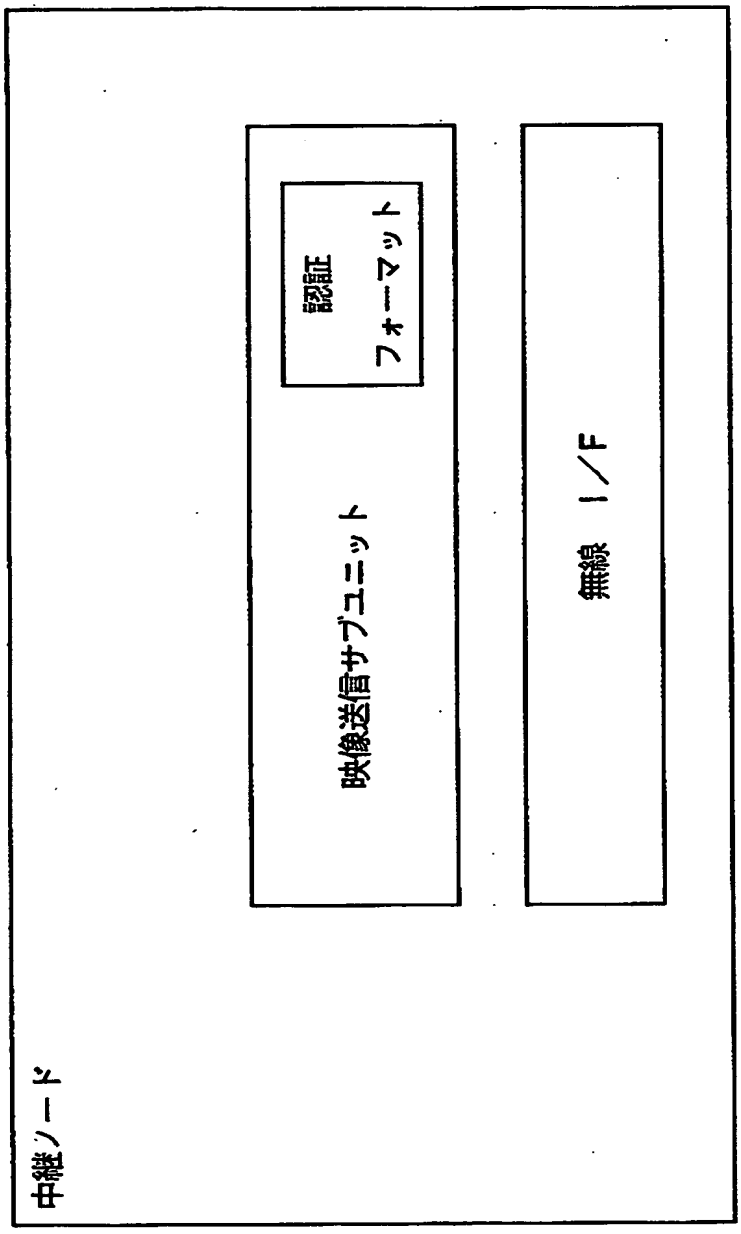

中継ノードが無線区間側に代理サービスする形態
映像送信サブユニット
.....
１３９４バス側の実体
送信ノード１０１の映像送信機能
（映像送信サブユニット）
.....

【図３５】

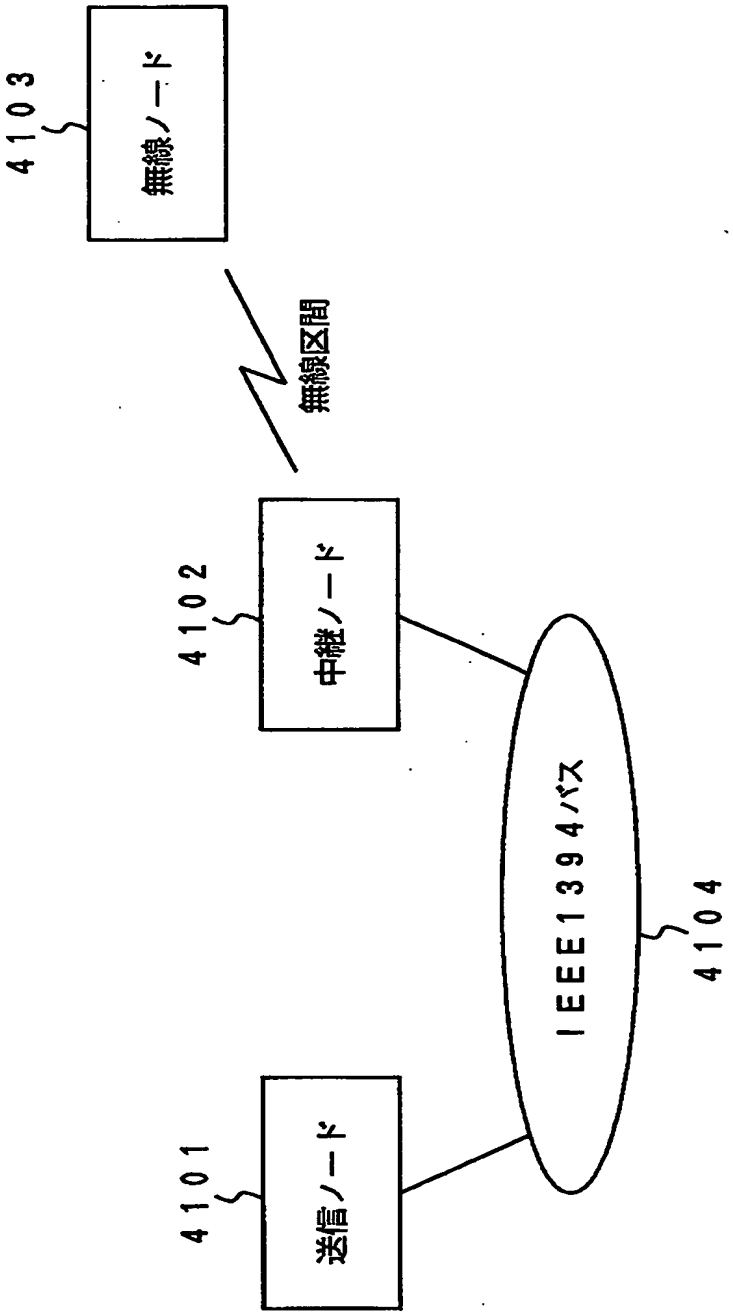


出証特平１１－３０２４２９１

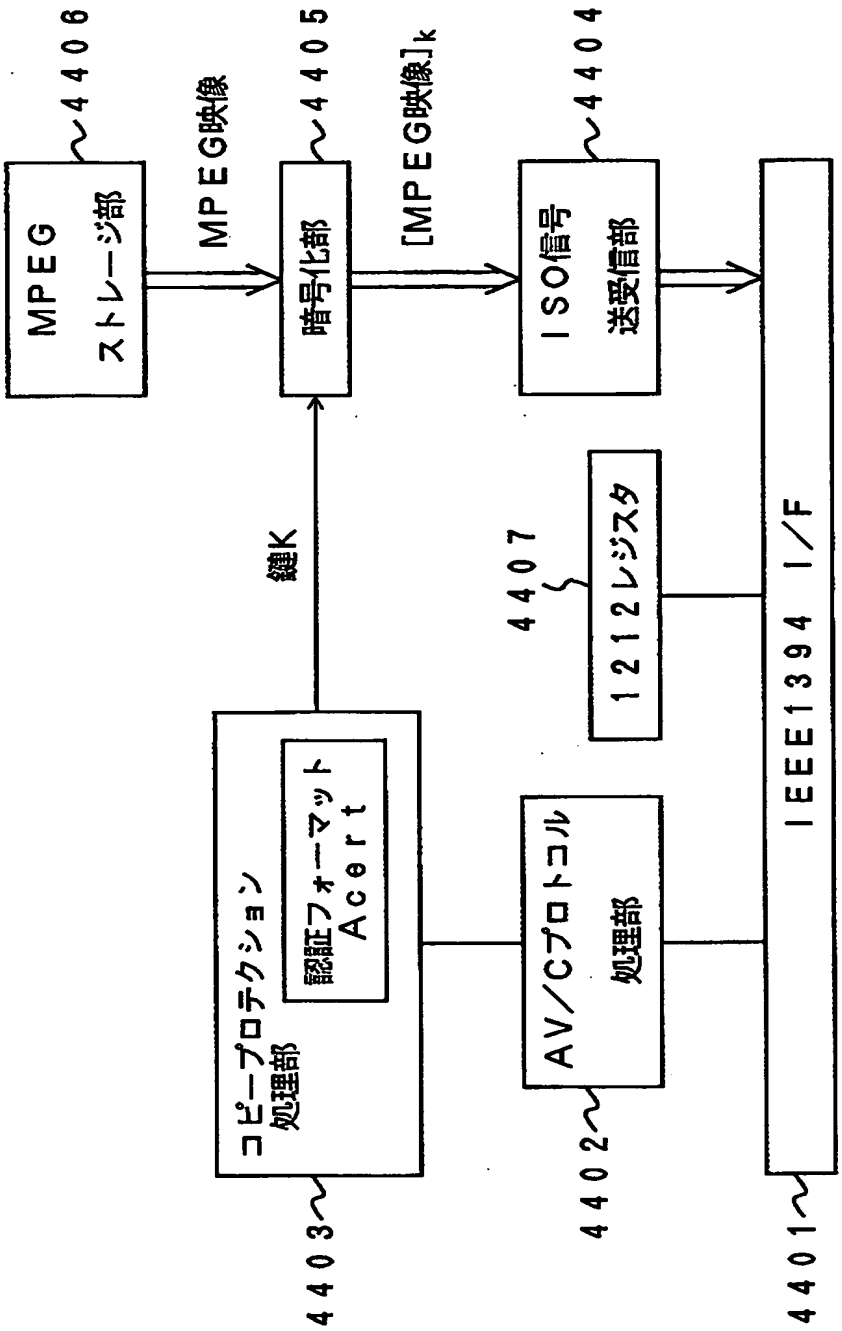
【図３６】



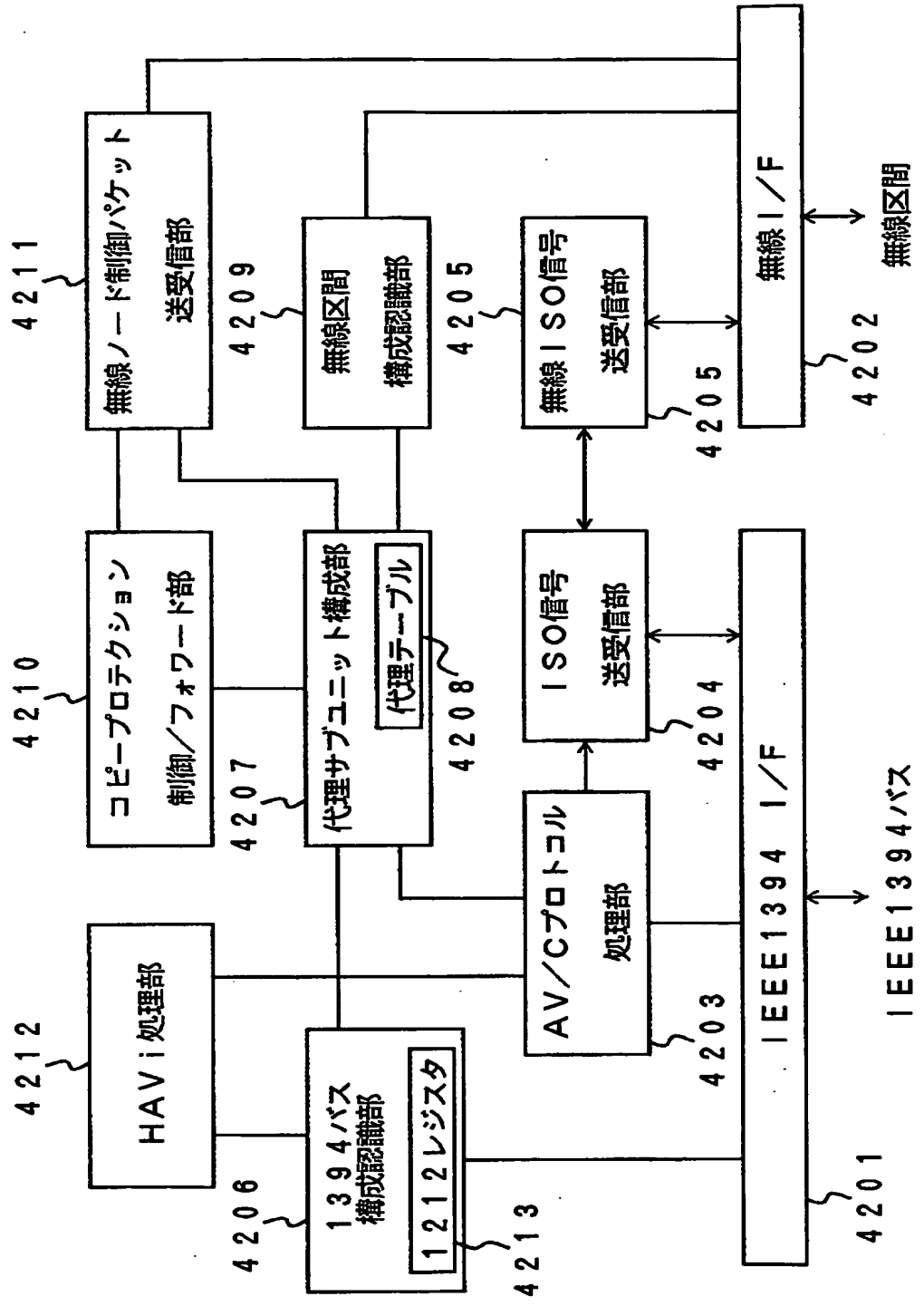
【図３７】



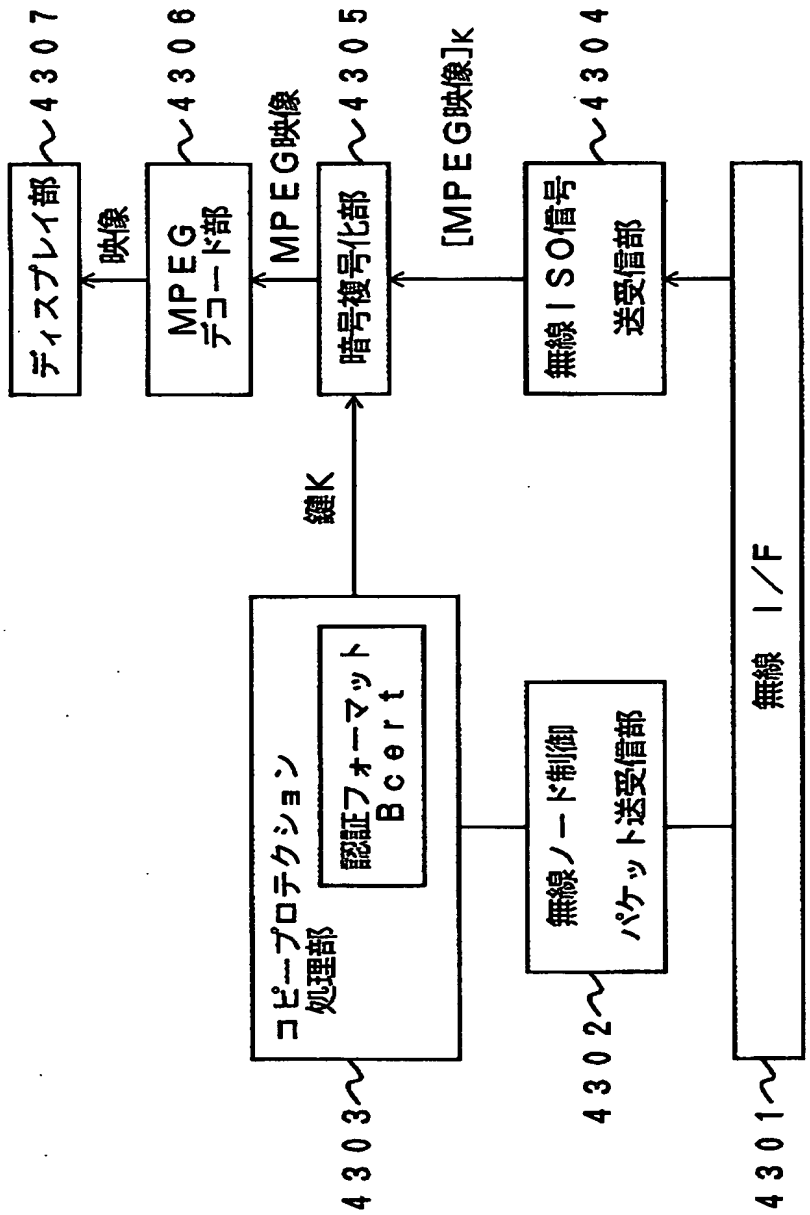
【図３８】


MPEG
ストレージ部
4406
MPEG映像
暗号化部
4405
[MPEG映像]k
ISO信号
送受信部
4404
鍵K
4407
1212レジスタ
IEEE1394 I/F
コピープロテクション
処理部
認証フォーマット
Acert
4403
AV/Cプロトコル
処理部
4402
4401

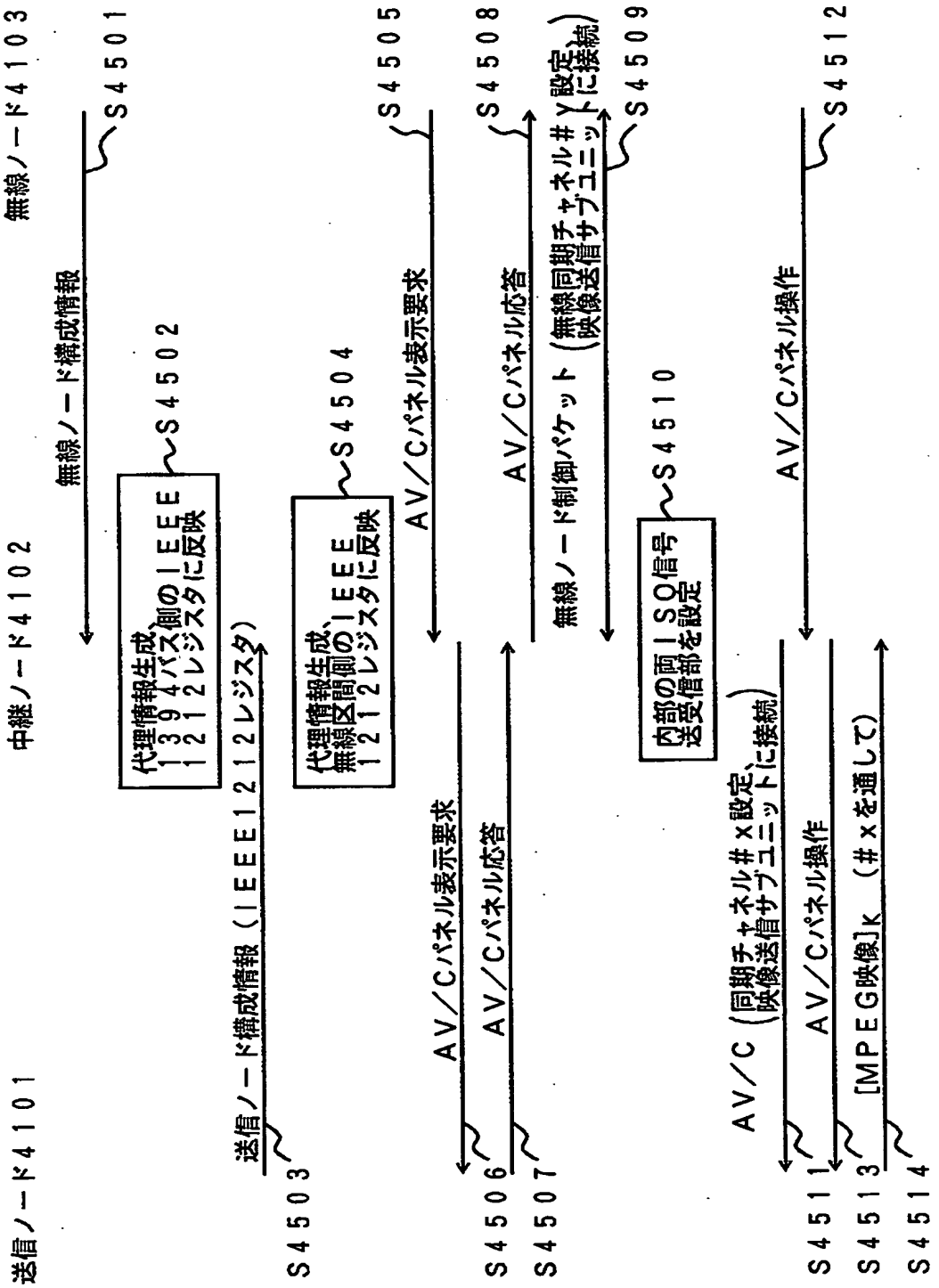
【図３９】


無線ノード制御パケット送受信部
4211
無線区間構成認識部
4209
無線ＩＳＯ信号送受信部
4205
無線Ｉ／Ｆ
4202
無線区間
コピープロテクション制御／フォワード部
4210
代理サブユニット構成部
代理テーブル
4208
4207
ＩＳＯ信号送受信部
4204
ＩＥＥＥ１３９４Ｉ／Ｆ
ＩＥＥＥ１３９４バス
HAVi処理部
4212
AV／Cプロトコル処理部
4203
1394バス構成認識部
1212レジスタ
4213
4206
4201

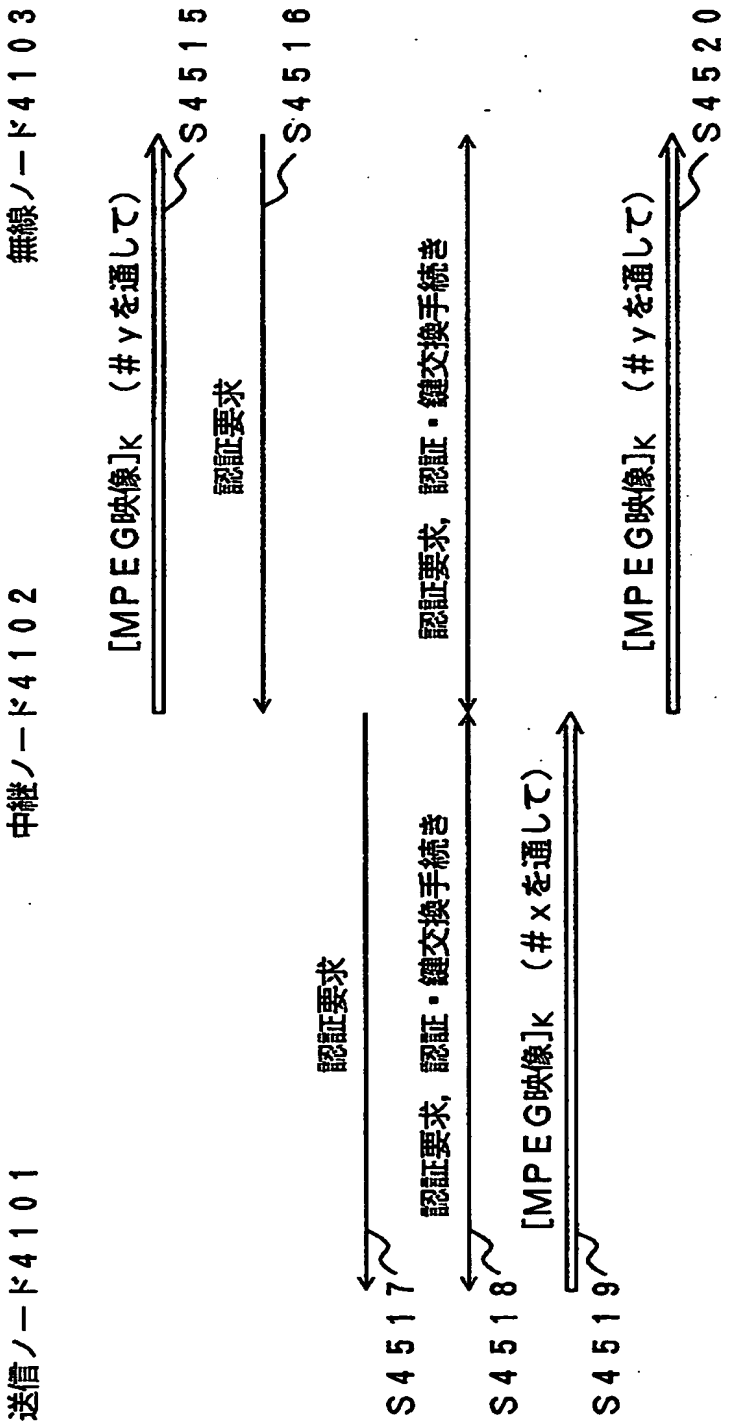
【図４０】


ディスプレイ部
4307
映像
MPEG
デコード部
4306
MPEG映像
暗号複号化部
4305
[MPEG映像]K
無線ISO信号
送受信部
4304
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
4303
無線ノード制御
パケット送受信部
4302
無線 I/F
4301

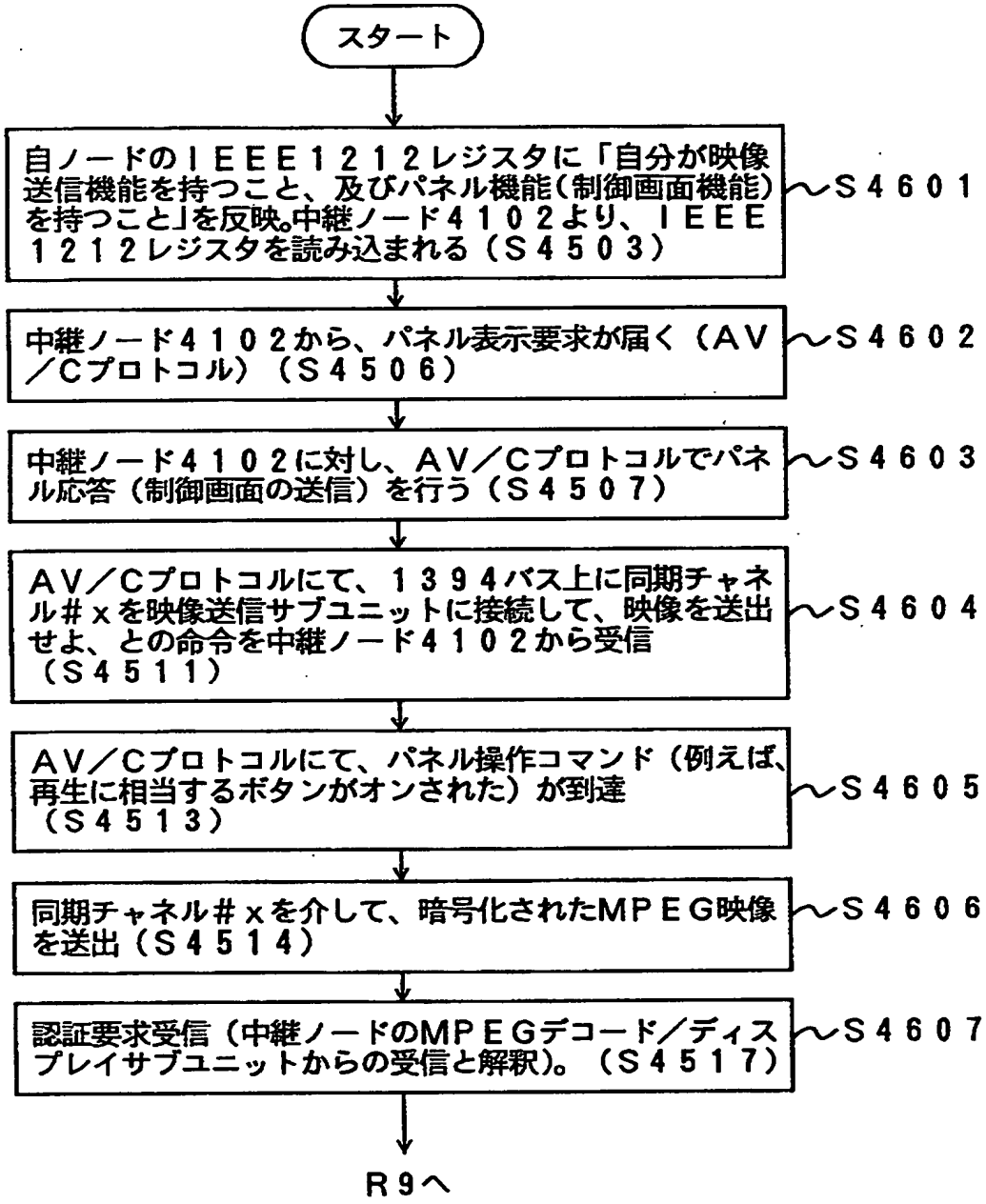
【図４１】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
無線ノード構成情報
S４５０１
代理情報生成、
１３９４バス側のＩＥＥＥ
１２１２レジスタに反映
S４５０２
送信ノード構成情報（ＩＥＥＥ１２１２レジスタ）
S４５０３
代理情報生成、
無線区間側のＩＥＥＥ
１２１２レジスタに反映
S４５０４
AV／Cパネル表示要求
S４５０５
AV／Cパネル表示要求
S４５０６
AV／Cパネル応答
S４５０７
AV／Cパネル応答
S４５０８
無線ノード制御パケット（無線同期チャネル＃Y設定、
映像送信サブユニットに接続）
S４５０９
内部のISO信号
送受信部を設定
S４５１０
AV／C（同期チャネル＃X設定、
映像送信サブユニットに接続）
S４５１１
AV／Cパネル操作
S４５１２
AV／Cパネル操作
S４５１３
[MPEG映像]K（＃Xを通して）
S４５１４

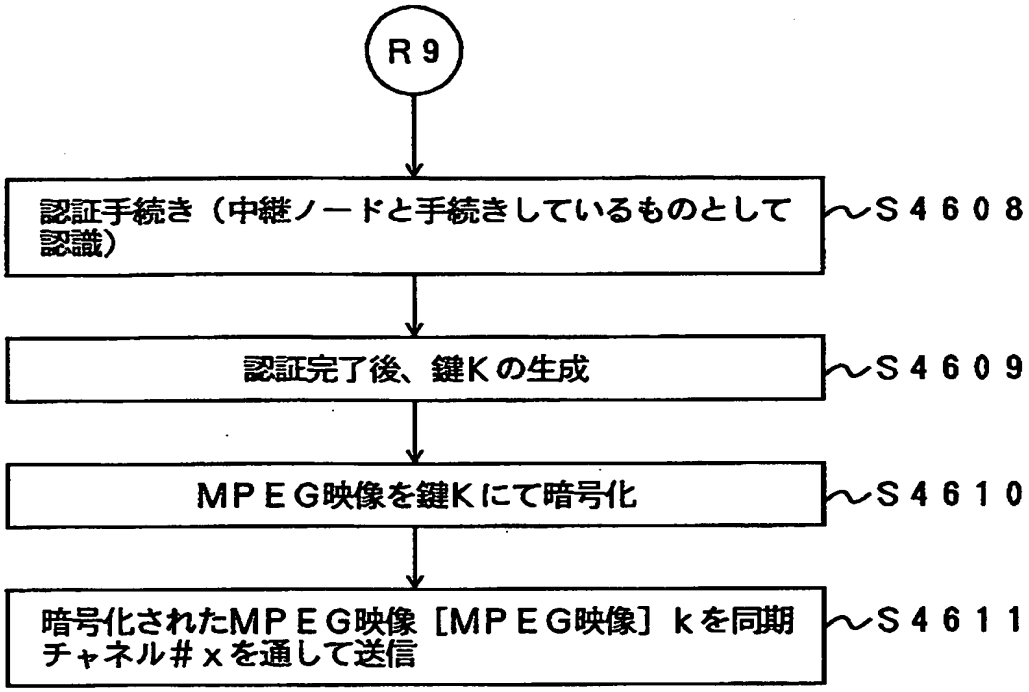
【図４２】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
[MPEG映像]K （#yを通して）
S４５１５
認証要求
S４５１６
[MPEG映像]K （#yを通して）
S４５２０
認証要求
S４５１７
認証要求，認証・鍵交換手続き
S４５１８
認証要求，認証・鍵交換手続き
[MPEG映像]K （#xを通して）
S４５１９

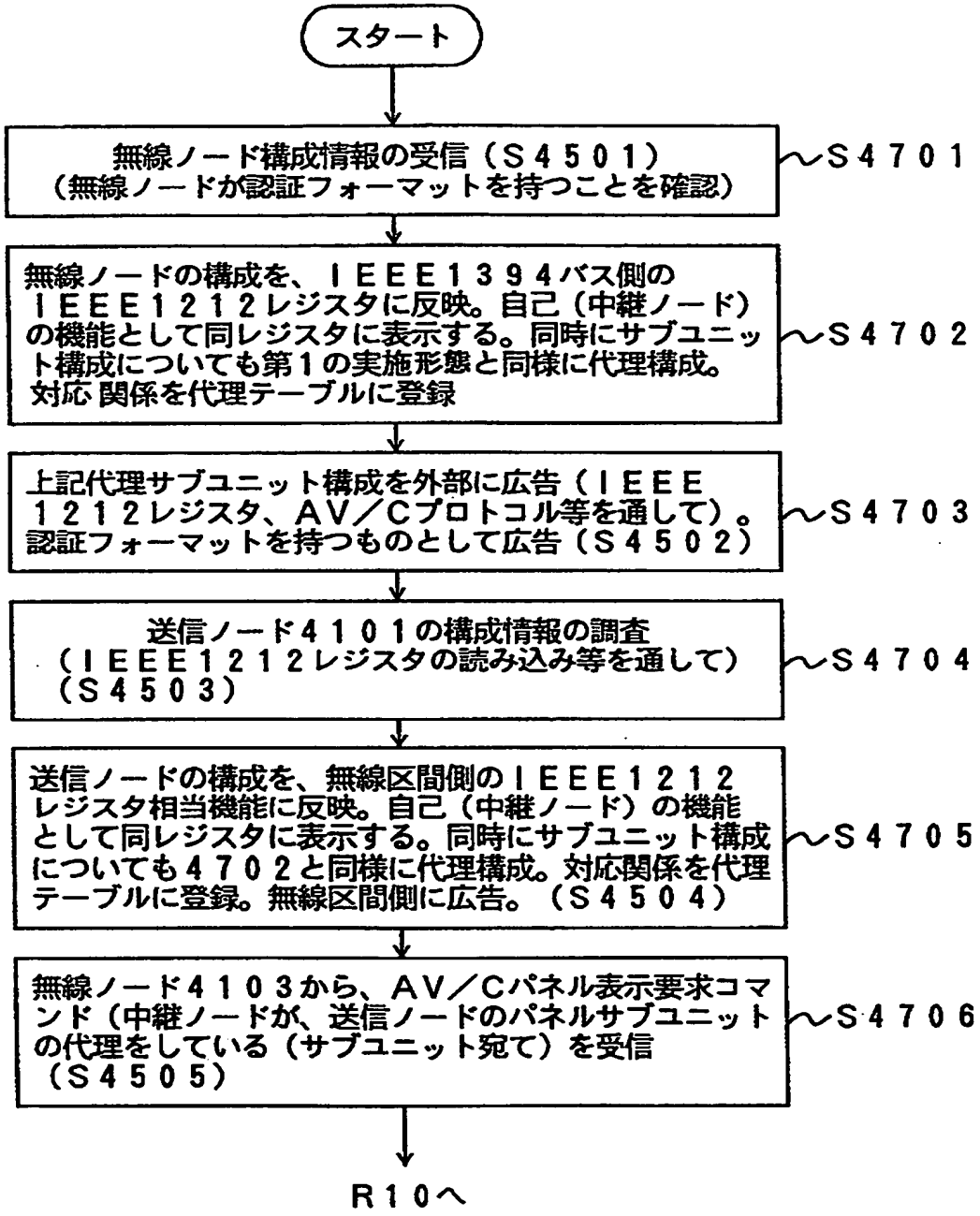
【図４３】


スタート
自ノードのＩＥＥＥ１２１２レジスタに「自分が映像送信機能を持つこと、及びパネル機能(制御画面機能)を持つこと」を反映。中継ノード４１０２より、ＩＥＥＥ１２１２レジスタを読み込まれる（Ｓ４５０３）
～Ｓ４６０１
中継ノード４１０２から、パネル表示要求が届く（ＡＶ／Ｃプロトコル）（Ｓ４５０６）
～Ｓ４６０２
中継ノード４１０２に対し、ＡＶ／Ｃプロトコルでパネル応答（制御画面の送信）を行う（Ｓ４５０７）
～Ｓ４６０３
ＡＶ／Ｃプロトコルにて、１３９４バス上に同期チャネル＃ｘを映像送信サブユニットに接続して、映像を送出せよ、との命令を中継ノード４１０２から受信（Ｓ４５１１）
～Ｓ４６０４
ＡＶ／Ｃプロトコルにて、パネル操作コマンド（例えば、再生に相当するボタンがオンされた）が到達（Ｓ４５１３）
～Ｓ４６０５
同期チャネル＃ｘを介して、暗号化されたＭＰＥＧ映像を送出（Ｓ４５１４）
～Ｓ４６０６
認証要求受信（中継ノードのＭＰＥＧデコード／ディスプレイサブユニットからの受信と解釈)。（Ｓ４５１７）
～Ｓ４６０７
Ｒ９へ

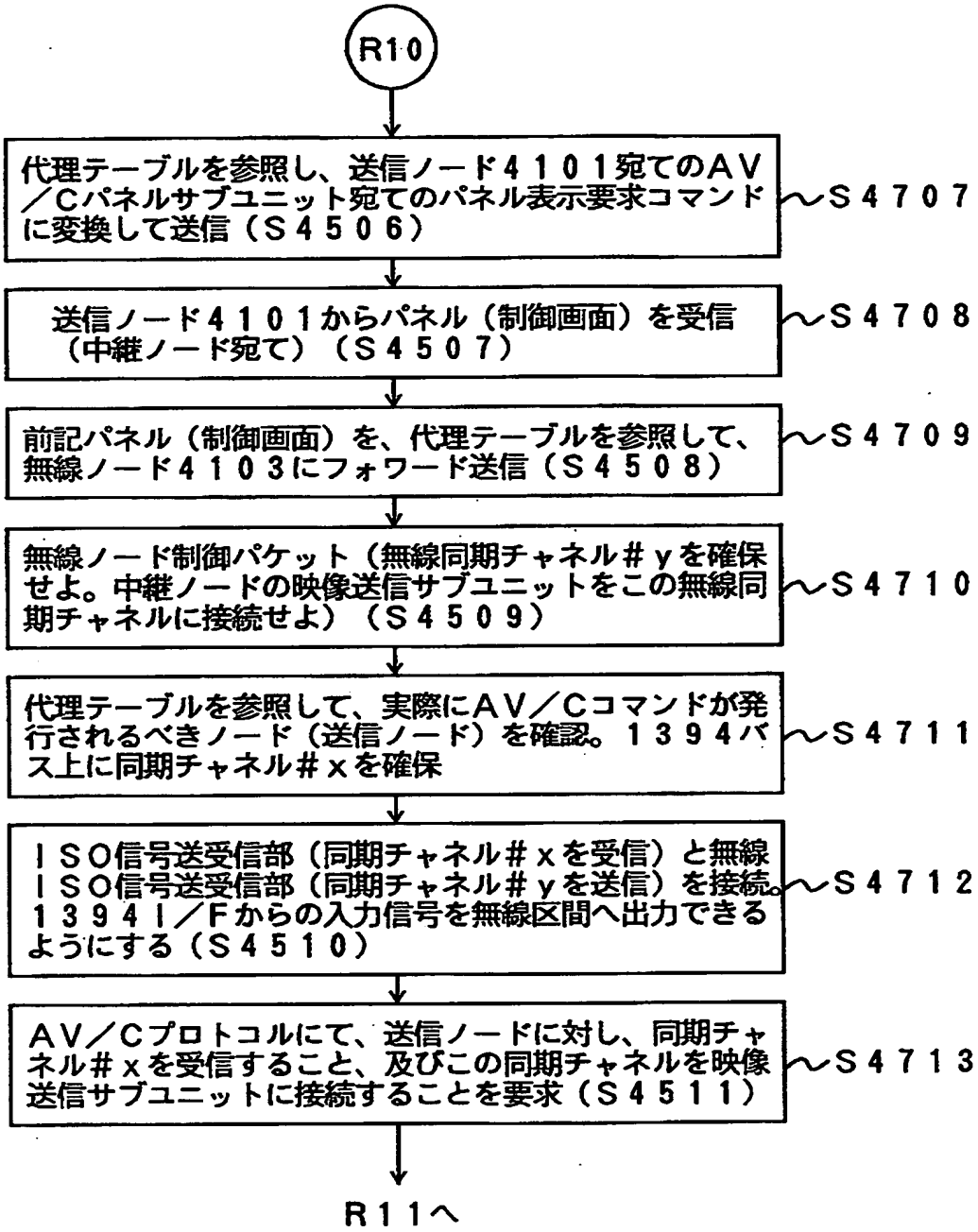
【図４４】


R9
認証手続き（中継ノードと手続きしているものとして認識）
S４６０８
認証完了後、鍵Kの生成
S４６０９
MPEG映像を鍵Kにて暗号化
S４６１０
暗号化されたMPEG映像［MPEG映像］kを同期チャネル#xを通して送信
S４６１１

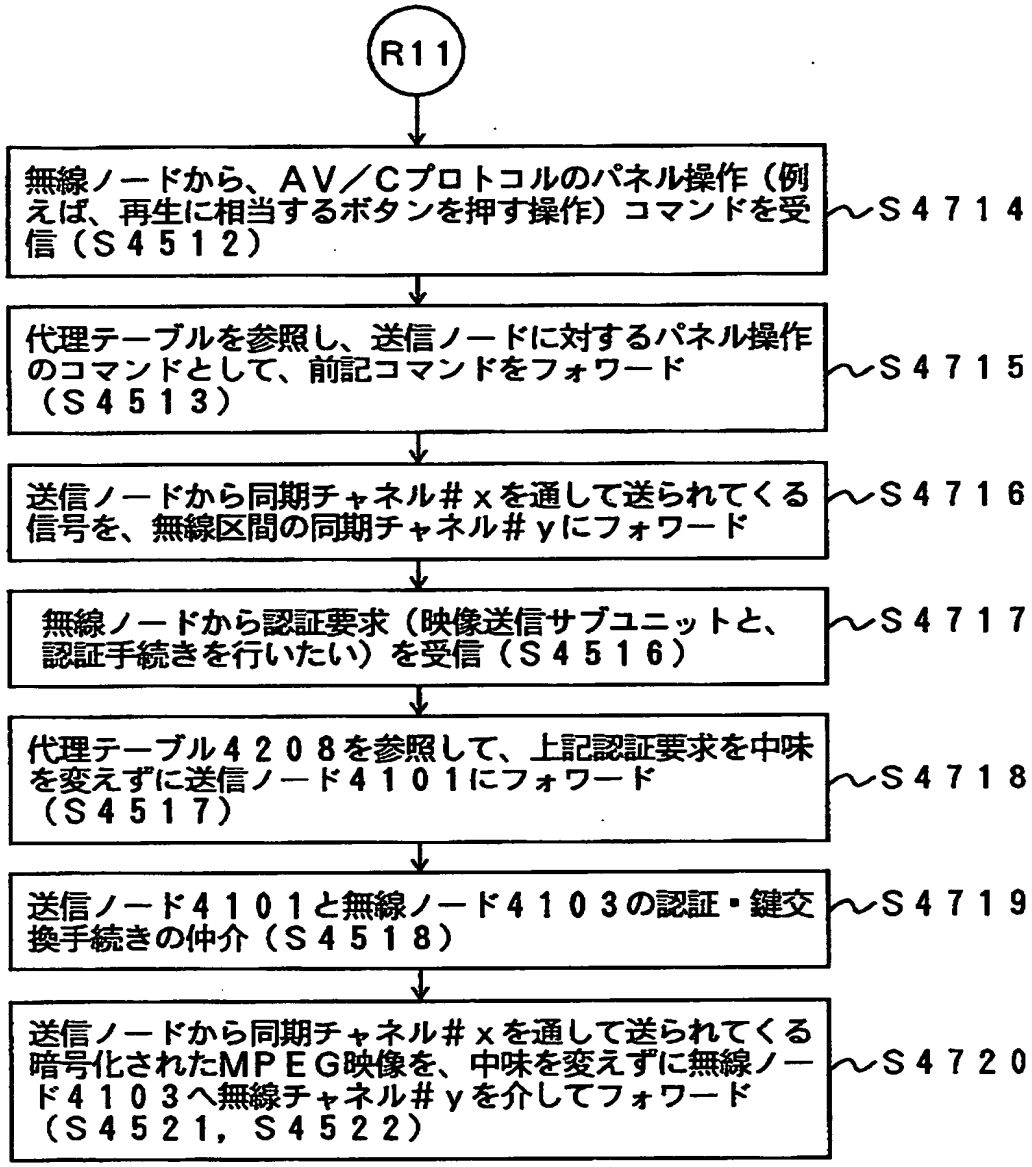
【図４５】


スタート
無線ノード構成情報の受信（Ｓ４５０１）
（無線ノードが認証フォーマットを持つことを確認）
～Ｓ４７０１
無線ノードの構成を、ＩＥＥＥ１３９４バス側のＩＥＥＥ１２１２レジスタに反映。自己（中継ノード）の機能として同レジスタに表示する。同時にサブユニット構成についても第１の実施形態と同様に代理構成。対応関係を代理テーブルに登録
～Ｓ４７０２
上記代理サブユニット構成を外部に広告（ＩＥＥＥ１２１２レジスタ、ＡＶ／Ｃプロトコル等を通して）。認証フォーマットを持つものとして広告（Ｓ４５０２）
～Ｓ４７０３
送信ノード４１０１の構成情報の調査
（ＩＥＥＥ１２１２レジスタの読み込み等を通して）
（Ｓ４５０３）
～Ｓ４７０４
送信ノードの構成を、無線区間側のＩＥＥＥ１２１２レジスタ相当機能に反映。自己（中継ノード）の機能として同レジスタに表示する。同時にサブユニット構成についても４７０２と同様に代理構成。対応関係を代理テーブルに登録。無線区間側に広告。（Ｓ４５０４）
～Ｓ４７０５
無線ノード４１０３から、ＡＶ／Ｃパネル表示要求コマンド（中継ノードが、送信ノードのパネルサブユニットの代理をしている（サブユニット宛て）を受信
（Ｓ４５０５）
～Ｓ４７０６
Ｒ１０へ

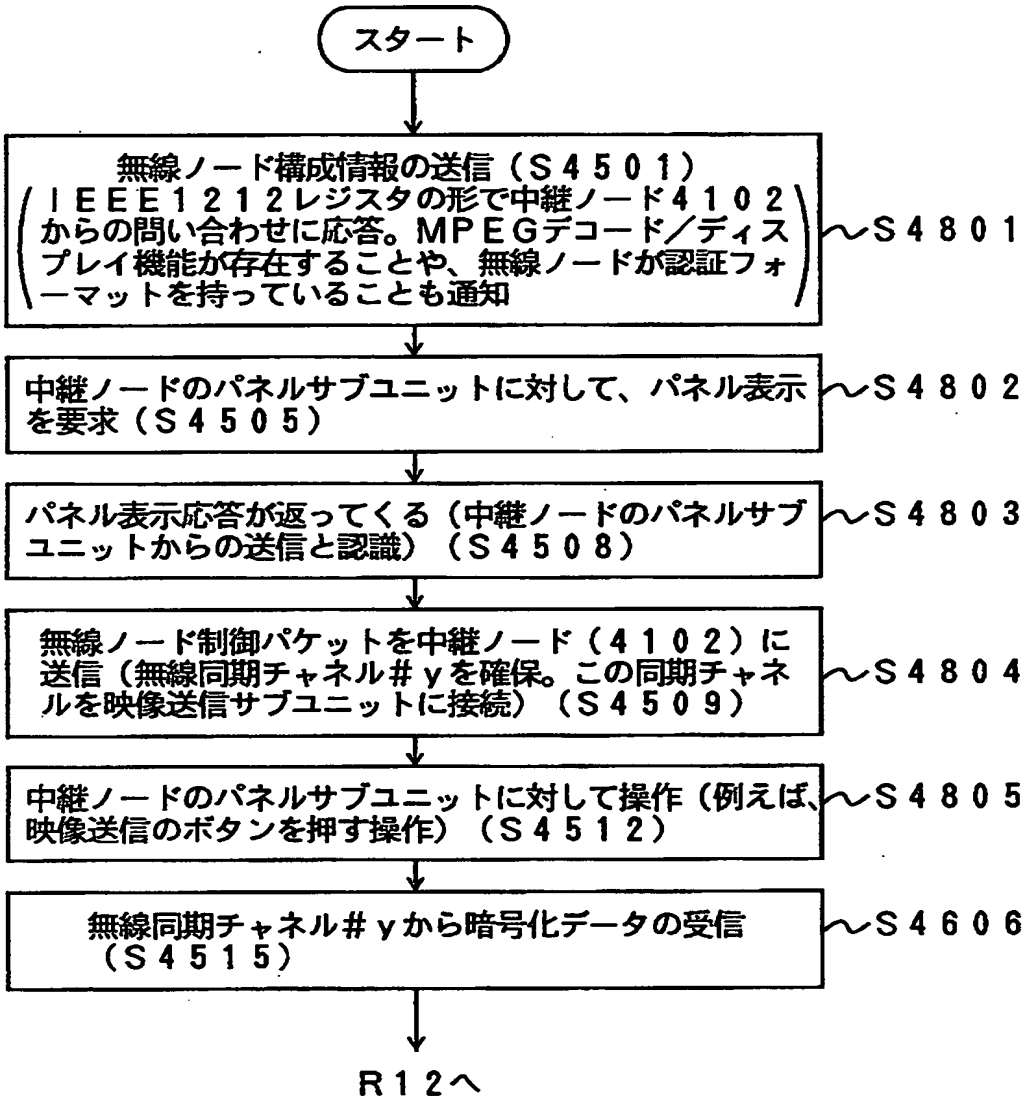
【図４６】


R10
代理テーブルを参照し、送信ノード４１０１宛てのＡＶ／Ｃパネルサブユニット宛てのパネル表示要求コマンドに変換して送信（Ｓ４５０６）
～Ｓ４７０７
送信ノード４１０１からパネル（制御画面）を受信（中継ノード宛て）（Ｓ４５０７）
～Ｓ４７０８
前記パネル（制御画面）を、代理テーブルを参照して、無線ノード４１０３にフォワード送信（Ｓ４５０８）
～Ｓ４７０９
無線ノード制御パケット（無線同期チャネル＃ｙを確保せよ。中継ノードの映像送信サブユニットをこの無線同期チャネルに接続せよ）（Ｓ４５０９）
～Ｓ４７１０
代理テーブルを参照して、実際にＡＶ／Ｃコマンドが発行されるべきノード（送信ノード）を確認。１３９４バス上に同期チャネル＃ｘを確保
～Ｓ４７１１
ＩＳＯ信号送受信部（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部（同期チャネル＃ｙを送信）を接続。１３９４Ｉ／Ｆからの入力信号を無線区間へ出力できるようにする（Ｓ４５１０）
～Ｓ４７１２
ＡＶ／Ｃプロトコルにて、送信ノードに対し、同期チャネル＃ｘを受信すること、及びこの同期チャネルを映像送信サブユニットに接続することを要求（Ｓ４５１１）
～Ｓ４７１３
R11へ

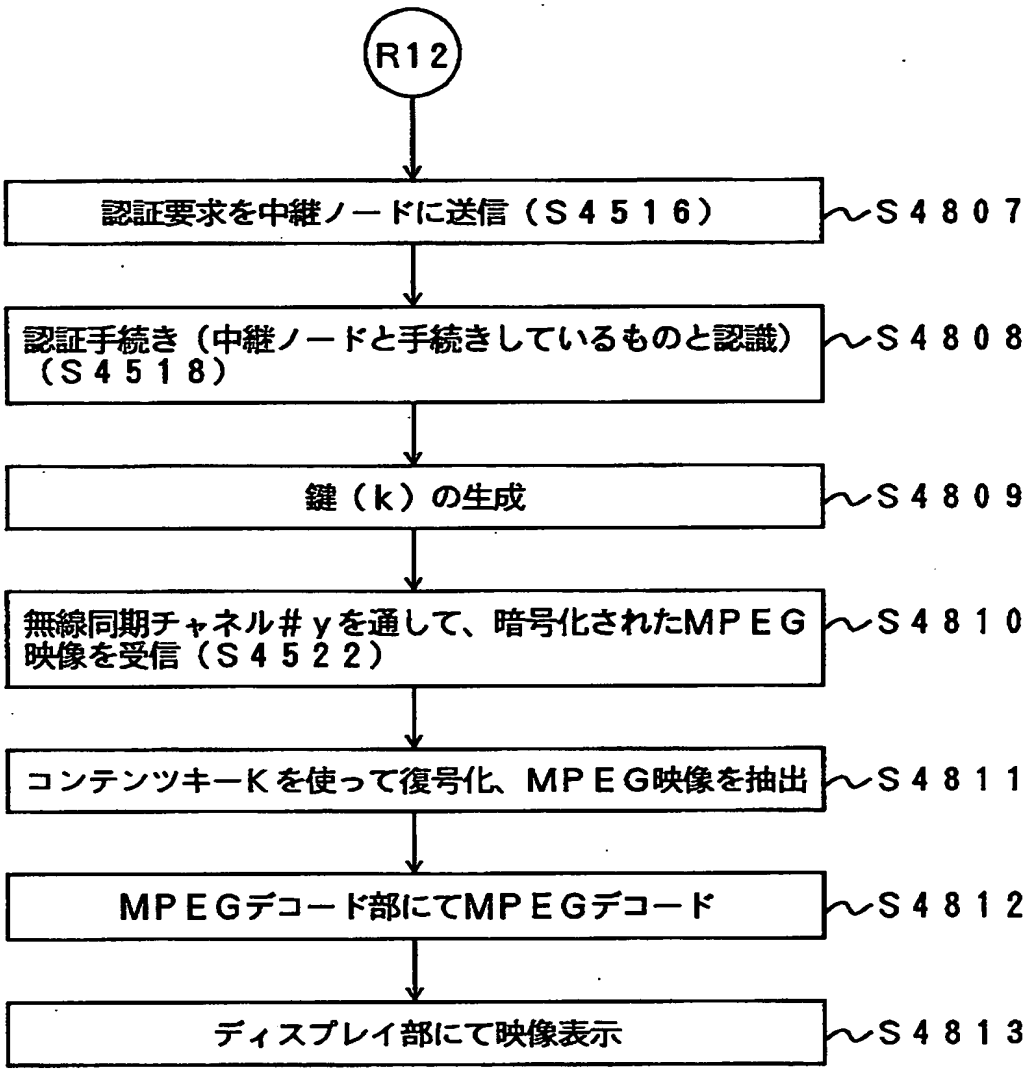
【図４７】


R11
無線ノードから、ＡＶ／Ｃプロトコルのパネル操作（例えば、再生に相当するボタンを押す操作）コマンドを受信（Ｓ４５１２）
Ｓ４７１４
代理テーブルを参照し、送信ノードに対するパネル操作のコマンドとして、前記コマンドをフォワード（Ｓ４５１３）
Ｓ４７１５
送信ノードから同期チャネル＃ｘを通して送られてくる信号を、無線区間の同期チャネル＃ｙにフォワード
Ｓ４７１６
無線ノードから認証要求（映像送信サブユニットと、認証手続きを行いたい）を受信（Ｓ４５１６）
Ｓ４７１７
代理テーブル４２０８を参照して、上記認証要求を中味を変えずに送信ノード４１０１にフォワード（Ｓ４５１７）
Ｓ４７１８
送信ノード４１０１と無線ノード４１０３の認証・鍵交換手続きの仲介（Ｓ４５１８）
Ｓ４７１９
送信ノードから同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、中味を変えずに無線ノード４１０３へ無線チャネル＃ｙを介してフォワード（Ｓ４５２１，Ｓ４５２２）
Ｓ４７２０

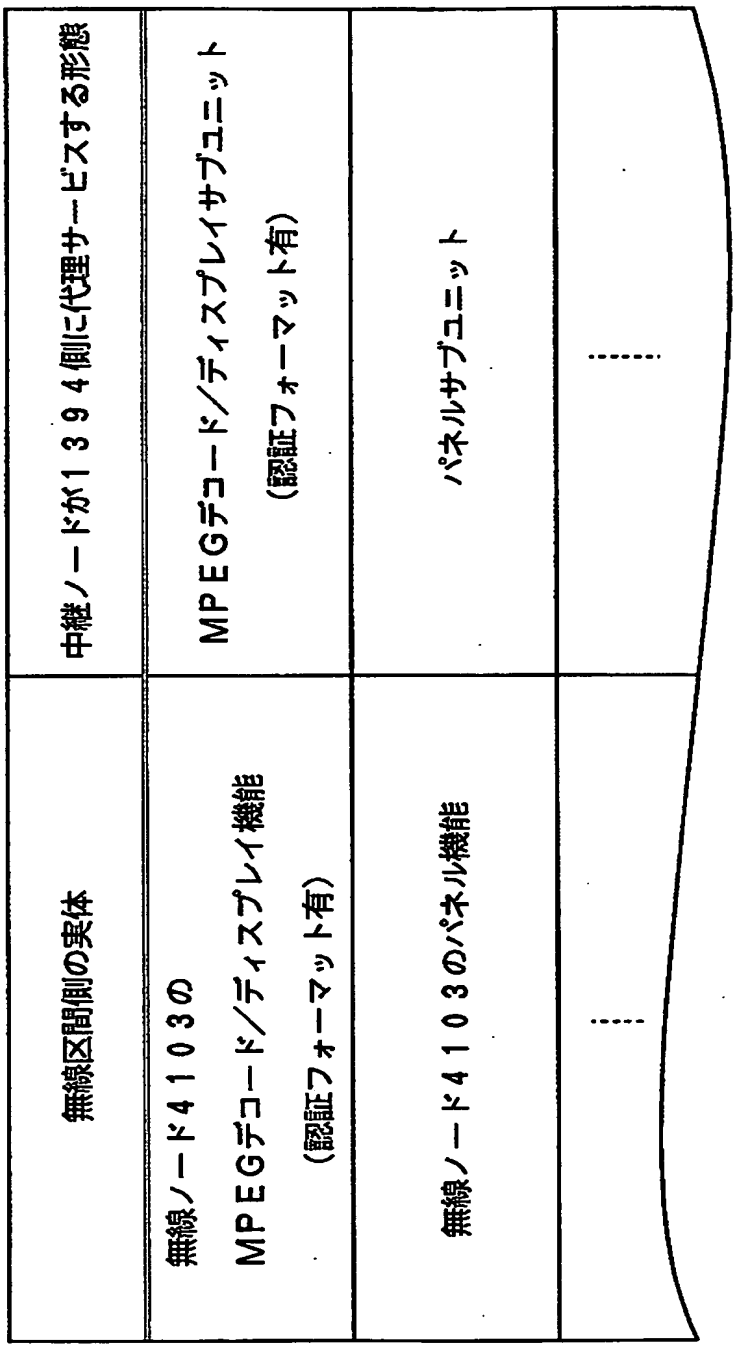
【図４８】


スタート
無線ノード構成情報の送信（Ｓ４５０１）
（ＩＥＥＥ１２１２レジスタの形で中継ノード４１０２からの問い合わせに応答。ＭＰＥＧデコード／ディスプレイ機能が存在することや、無線ノードが認証フォーマットを持っていることも通知）
～Ｓ４８０１
中継ノードのパネルサブユニットに対して、パネル表示を要求（Ｓ４５０５）
～Ｓ４８０２
パネル表示応答が返ってくる（中継ノードのパネルサブユニットからの送信と認識）（Ｓ４５０８）
～Ｓ４８０３
無線ノード制御パケットを中継ノード（４１０２）に送信（無線同期チャネル＃ｙを確保。この同期チャネルを映像送信サブユニットに接続）（Ｓ４５０９）
～Ｓ４８０４
中継ノードのパネルサブユニットに対して操作（例えば、映像送信のボタンを押す操作）（Ｓ４５１２）
～Ｓ４８０５
無線同期チャネル＃ｙから暗号化データの受信（Ｓ４５１５）
～Ｓ４６０６
Ｒ１２へ

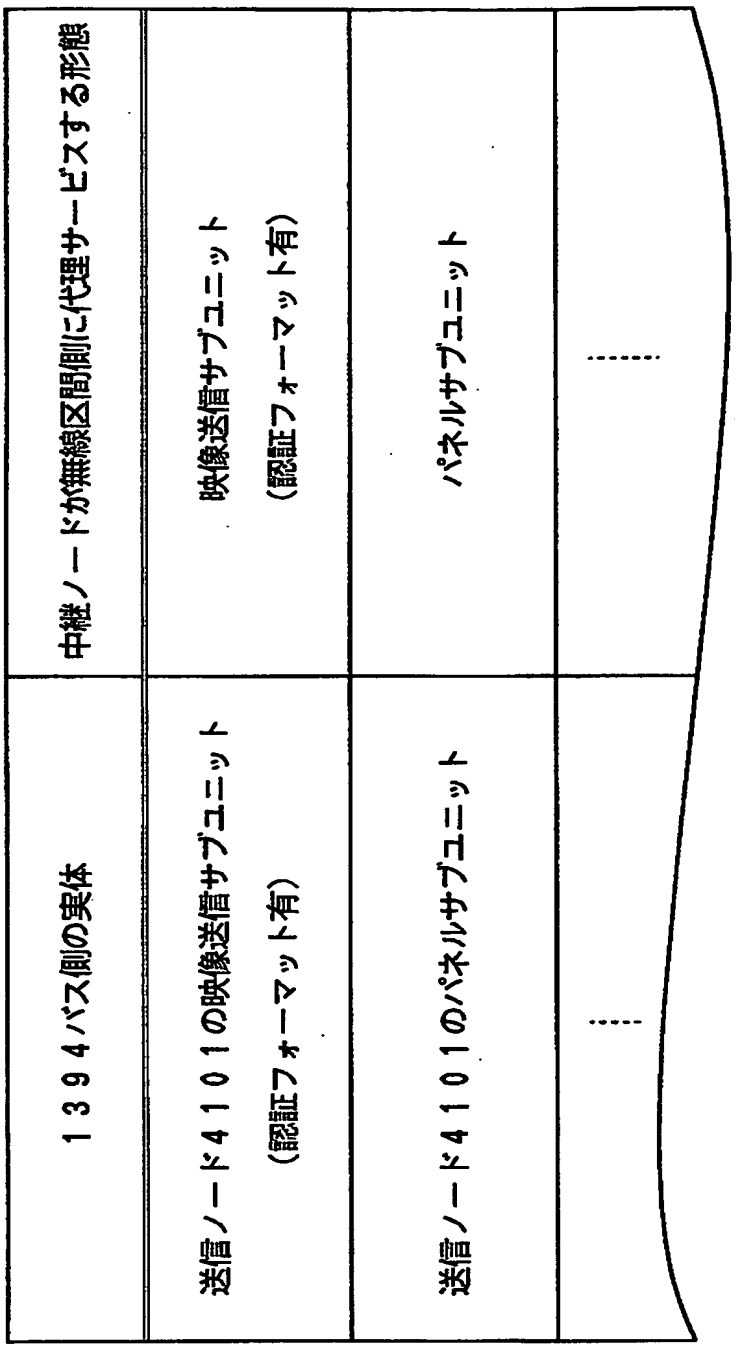
【図４９】


R12
認証要求を中継ノードに送信（Ｓ４５１６）
Ｓ４８０７
認証手続き（中継ノードと手続きしているものと認識）（Ｓ４５１８）
Ｓ４８０８
鍵（ｋ）の生成
Ｓ４８０９
無線同期チャネル＃ｙを通して、暗号化されたＭＰＥＧ映像を受信（Ｓ４５２２）
Ｓ４８１０
コンテンツキーＫを使って復号化、ＭＰＥＧ映像を抽出
Ｓ４８１１
ＭＰＥＧデコード部にてＭＰＥＧデコード
Ｓ４８１２
ディスプレイ部にて映像表示
Ｓ４８１３

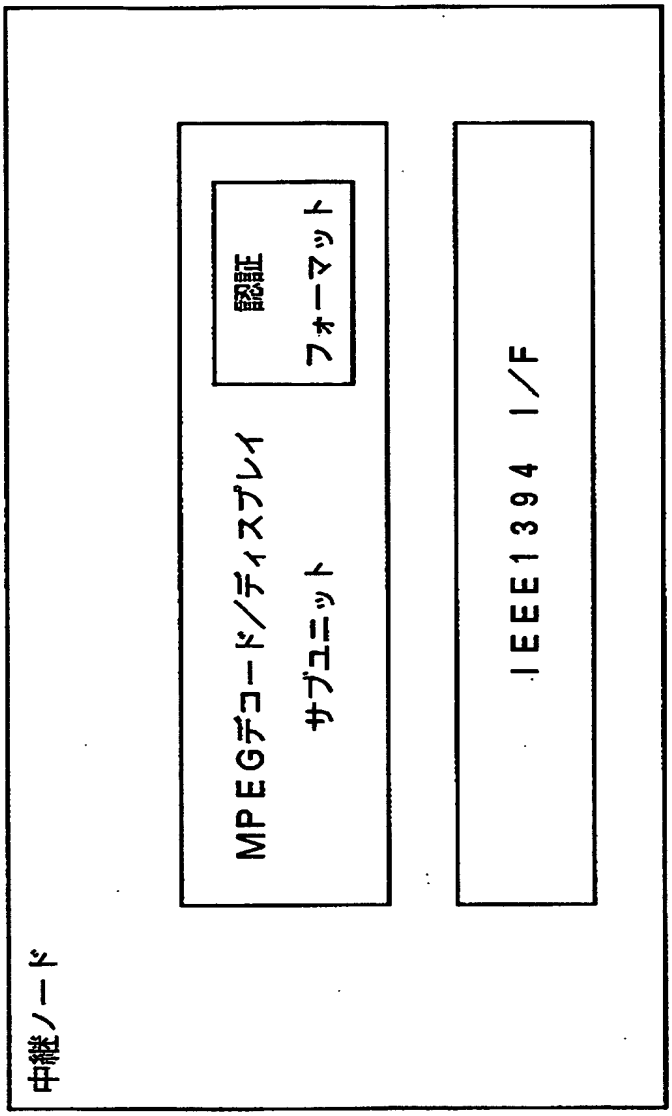
【図５０】


無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード４１０３の
MPEGデコード／ディスプレイ機能
（認証フォーマット有）
MPEGデコード／ディスプレイサブユニット
（認証フォーマット有）
無線ノード４１０３のパネル機能
パネルサブユニット

【図５１】

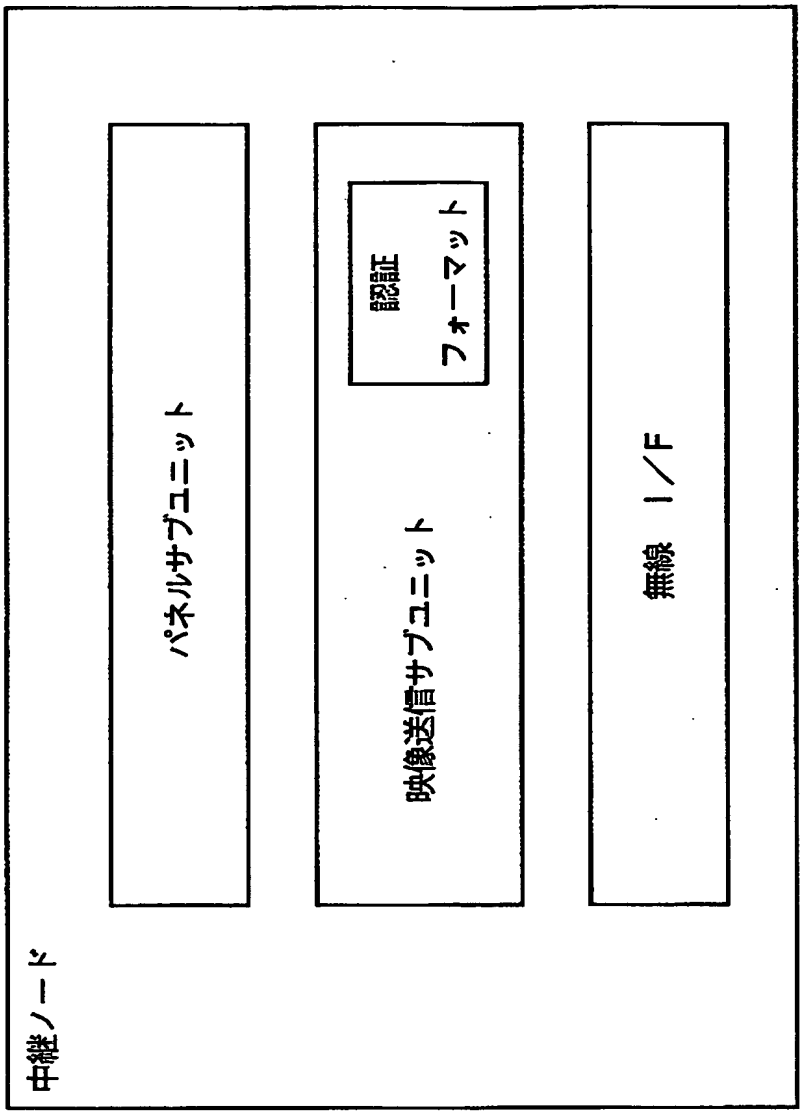

１３９４バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード４１０１の映像送信サブユニット
（認証フォーマット有）
映像送信サブユニット
（認証フォーマット有）
送信ノード４１０１のパネルサブユニット
パネルサブユニット

【図５２】



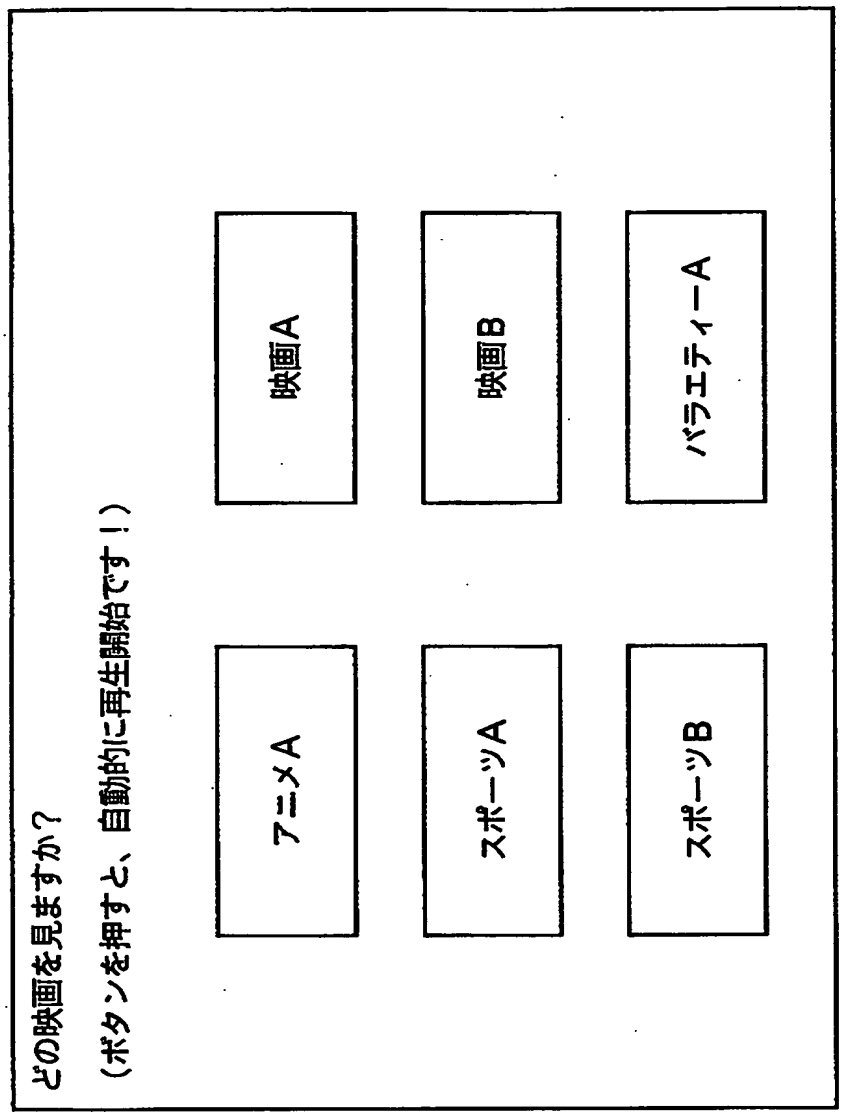
出証特平１１－３０２４２９１

【図５３】



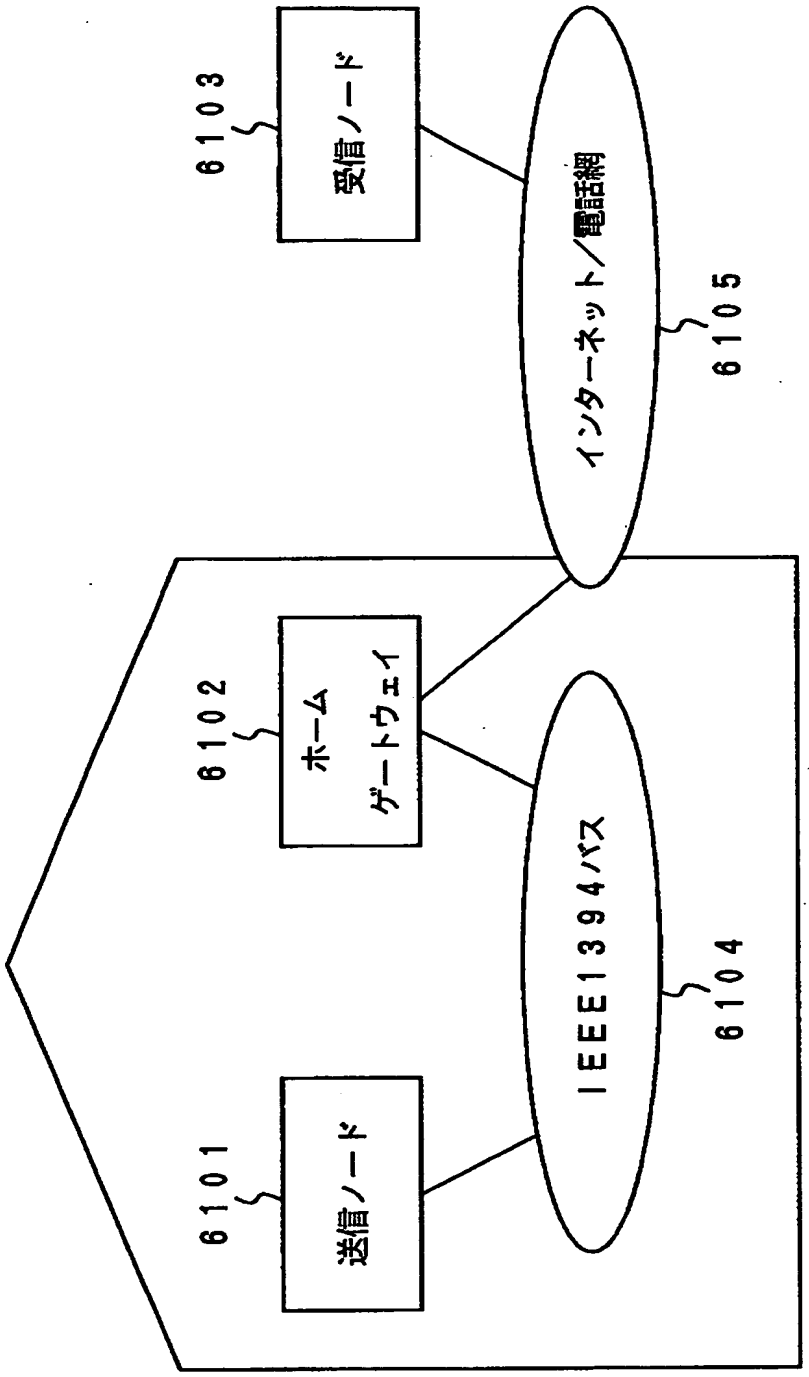
出証特平１１－３０２４２９１

【図５４】

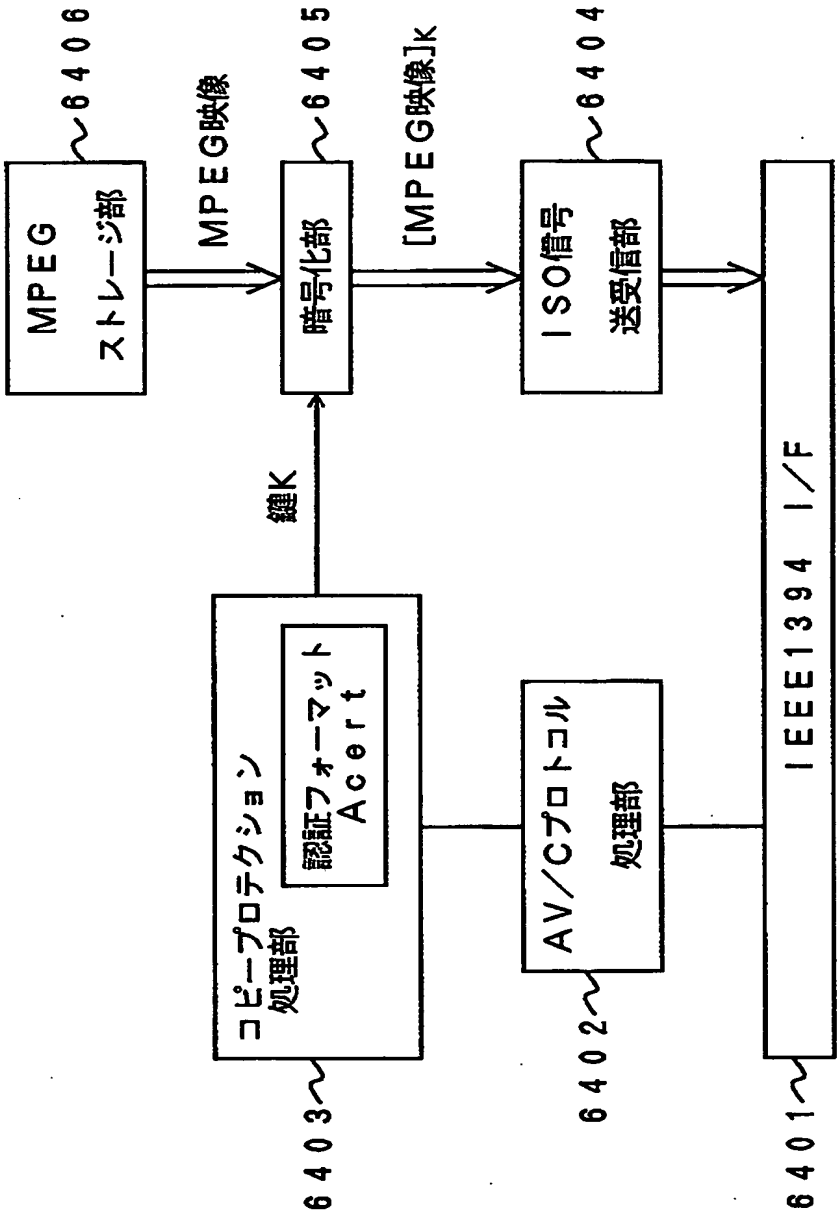


出証特平１１－３０２４２９１

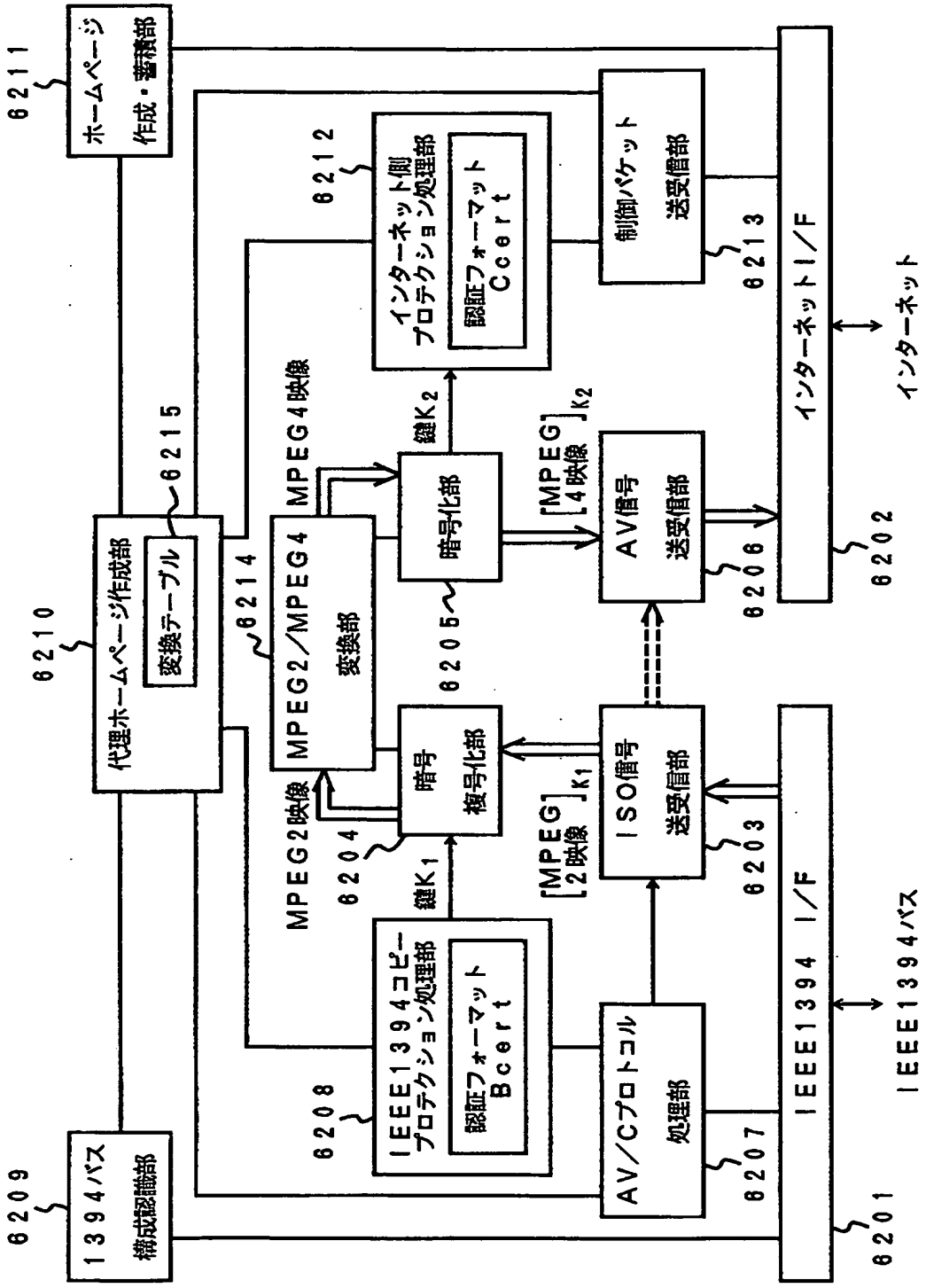
【図５５】


6103
受信ノード
インターネット／電話網
6105
6102
ホーム
ゲートウェイ
IEEE1394バス
6104
6101
送信ノード

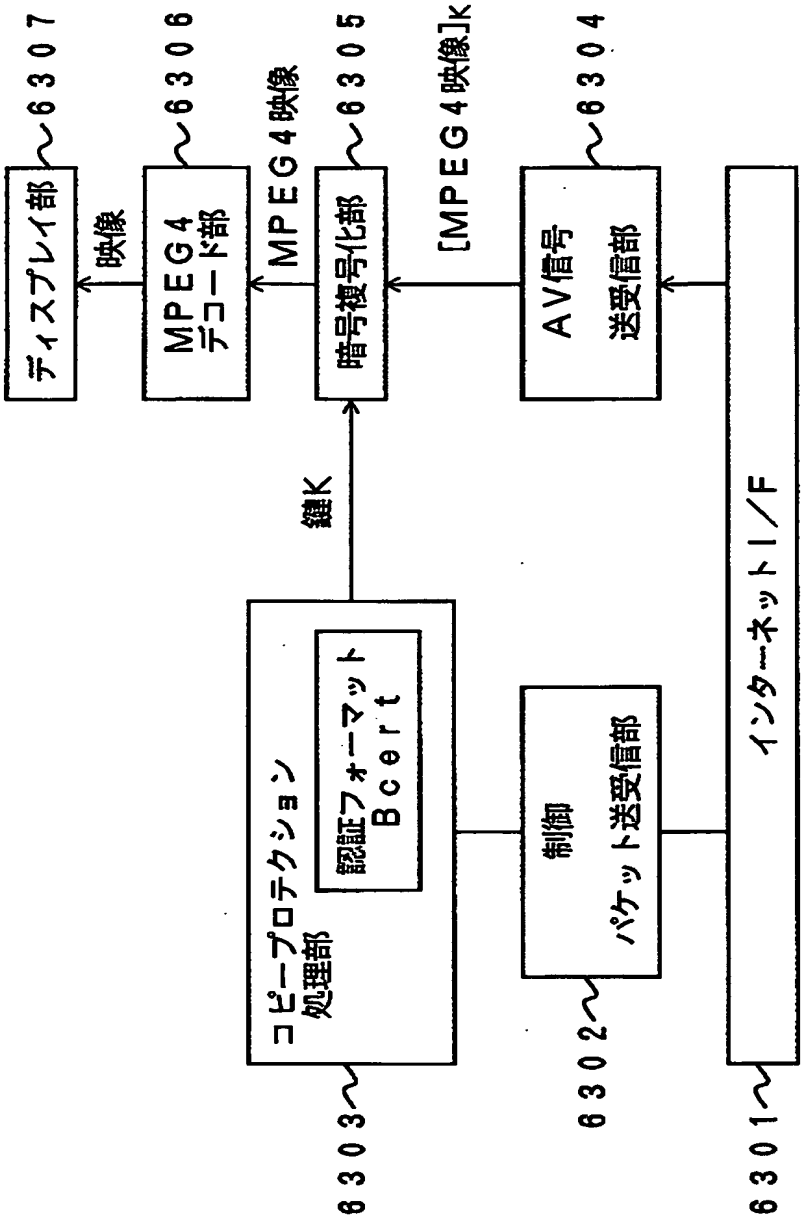
【図５６】


MPEG
ストレージ部
6406
MPEG映像
暗号化部
6405
[MPEG映像]K
ISO信号
送受信部
6404
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
6403
AV/Cプロトコル
処理部
6402
IEEE1394 I/F
6401

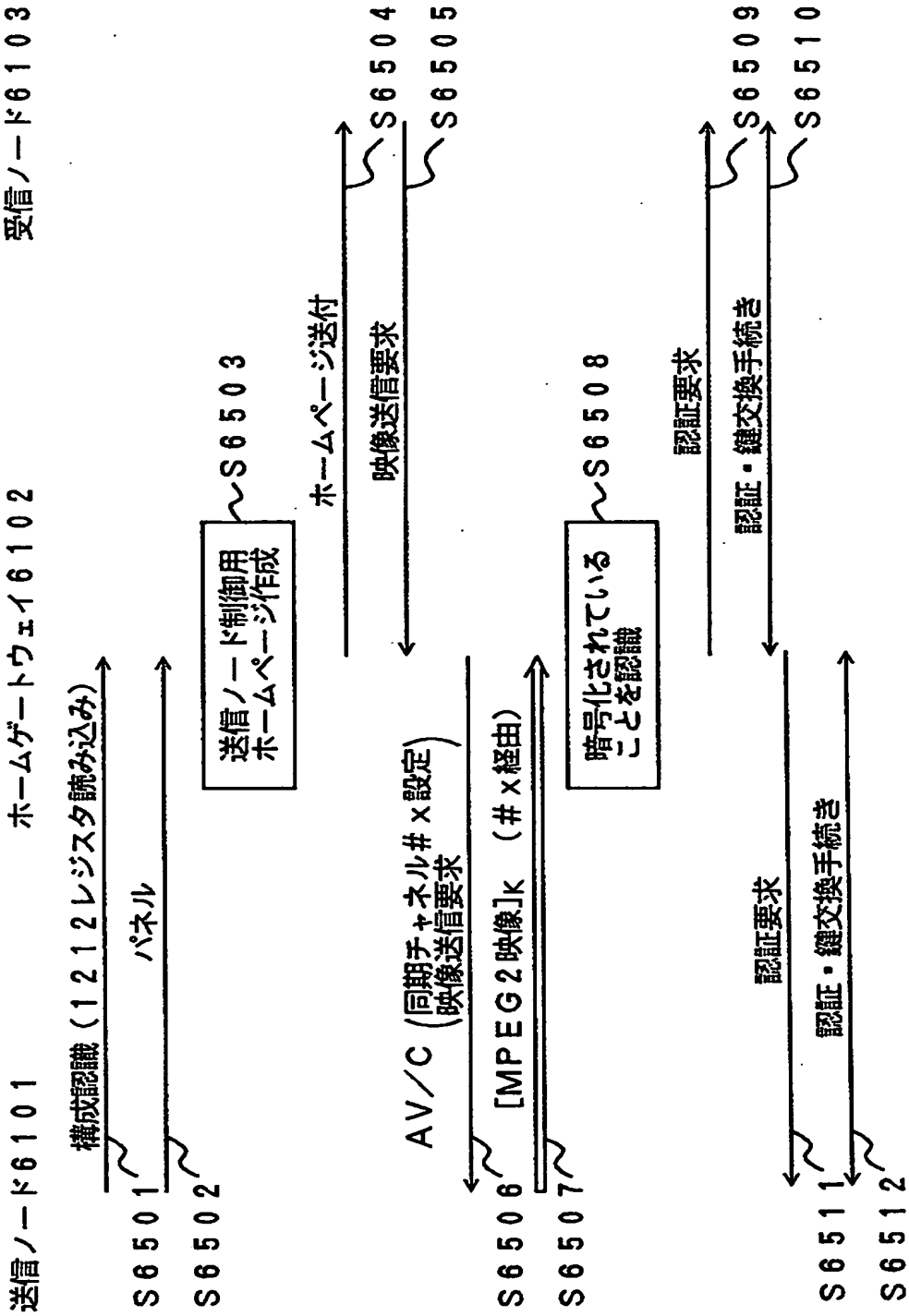
【図５７】


6211
ホームページ
作成・蓄積部
6212
インターネット側
プロテクション処理部
認証フォーマット
Ccert
制御パケット
送受信部
6213
インターネットI／F
6202
インターネット
6215
代理ホームページ作成部
変換テーブル
6210
MPEG4映像
MPEG2／MPEG4
変換部
6214
鍵K2
暗号化部
6205
[MPEG
[4映像]K2
AV信号
送受信部
6206
MPEG2映像
6204
暗号
複号化部
鍵K1
[MPEG
[2映像]K1
ISO信号
送受信部
6203
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
6208
AV／Cプロトコル
処理部
6207
IEEE1394 I／F
6201
IEEE1394バス
6209
1394バス
機成認識部

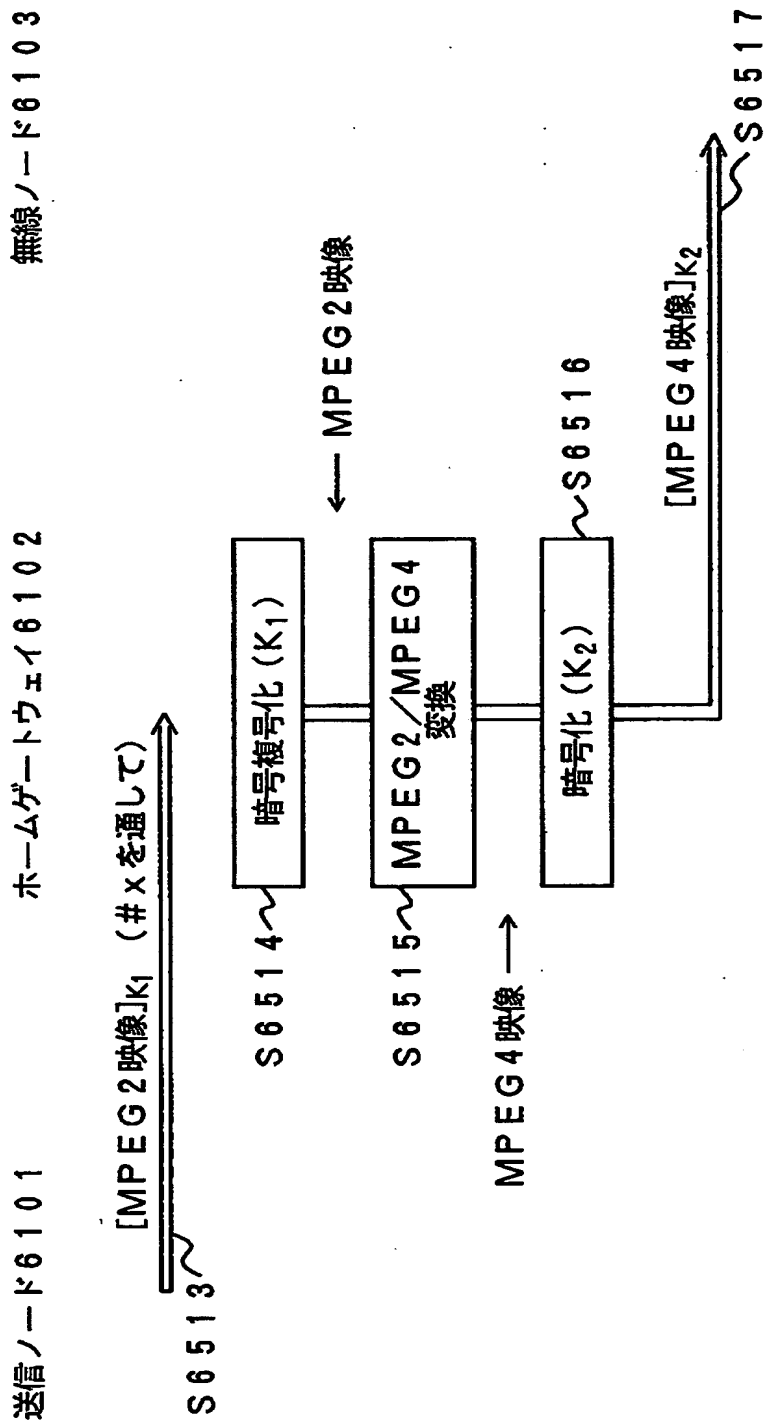
【図５８】


ディスプレイ部
6307
映像
MPEG4
デコード部
6306
MPEG4映像
暗号複号化部
6305
[MPEG4映像]k
AV信号
送受信部
6304
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
6303
制御
パケット送受信部
6302
インターネットI／F
6301

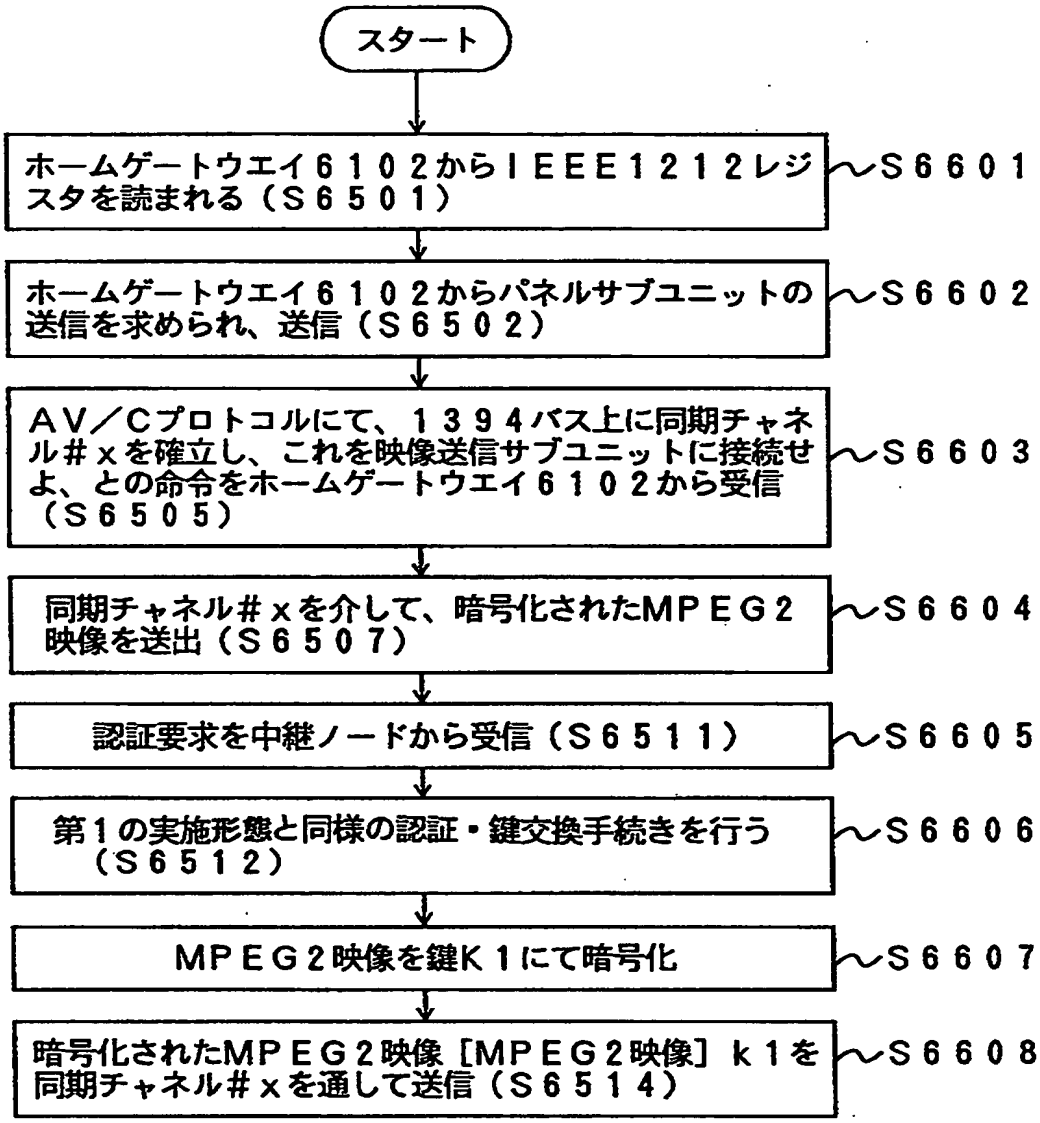
【図５９】


送信ノード6101
ホームゲートウェイ6102
受信ノード6103
構成認識（1212レジスタ読み込み）
パネル
S6501
S6502
送信ノード制御用
ホームページ作成
S6503
ホームページ送付
S6504
映像送信要求
S6505
AV／C（同期チャネル#x設定
映像送信要求）
[MPEG2映像]K（#x経由）
S6506
S6507
暗号化されている
ことを認識
S6508
認証要求
S6509
認証・鍵交換手続き
S6510
認証要求
認証・鍵交換手続き
S6511
S6512

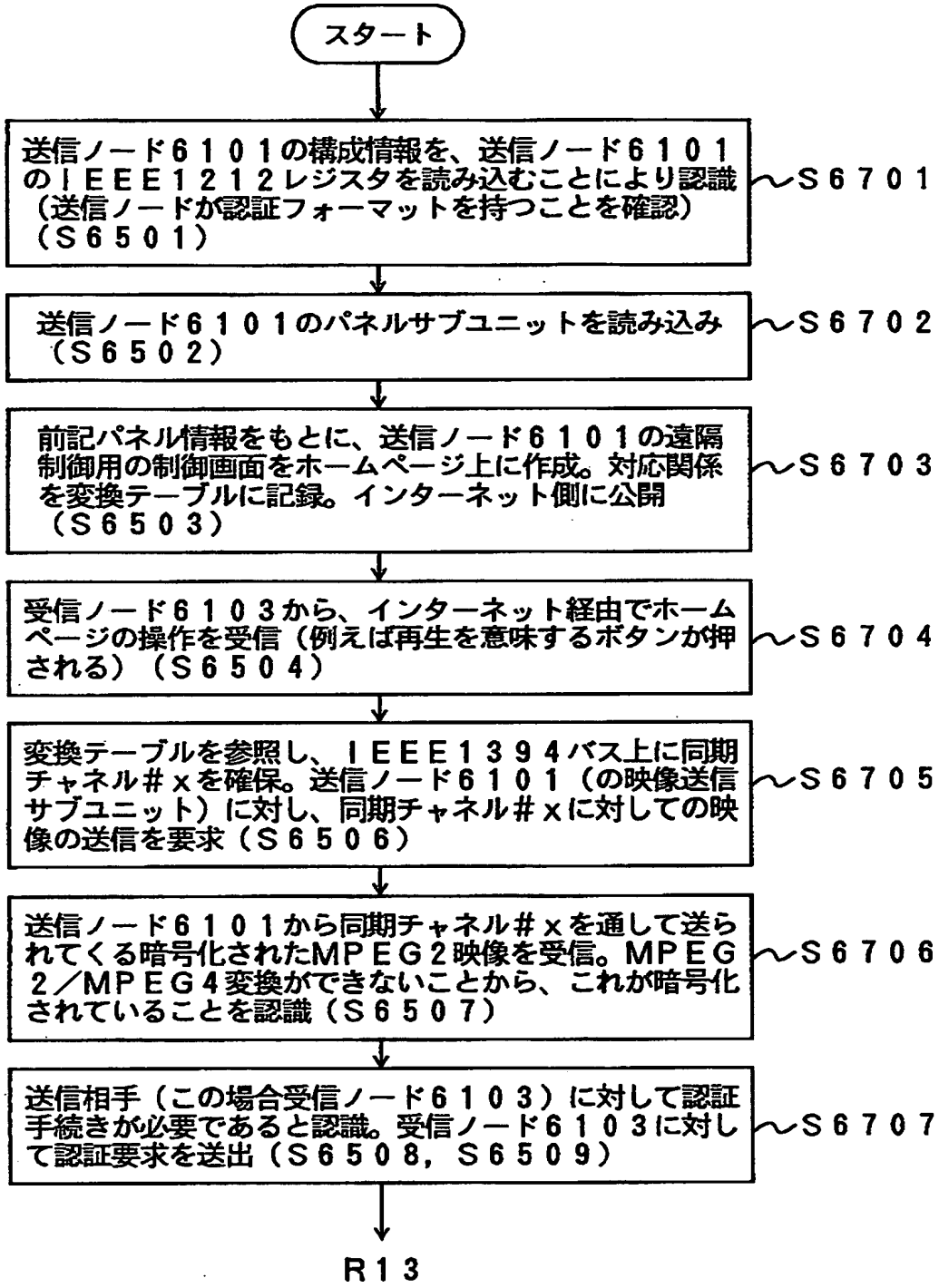
【図６０】


送信ノード６１０１
ホームゲートウェイ６１０２
無線ノード６１０３
[MPEG2映像]K1 （#xを通して）
S6513
暗号複号化（K1）
S6514
MPEG2／MPEG4 変換
S6515
暗号化（K2）
S6516
[MPEG4映像]K2
S6517
← MPEG2映像
MPEG4映像 →

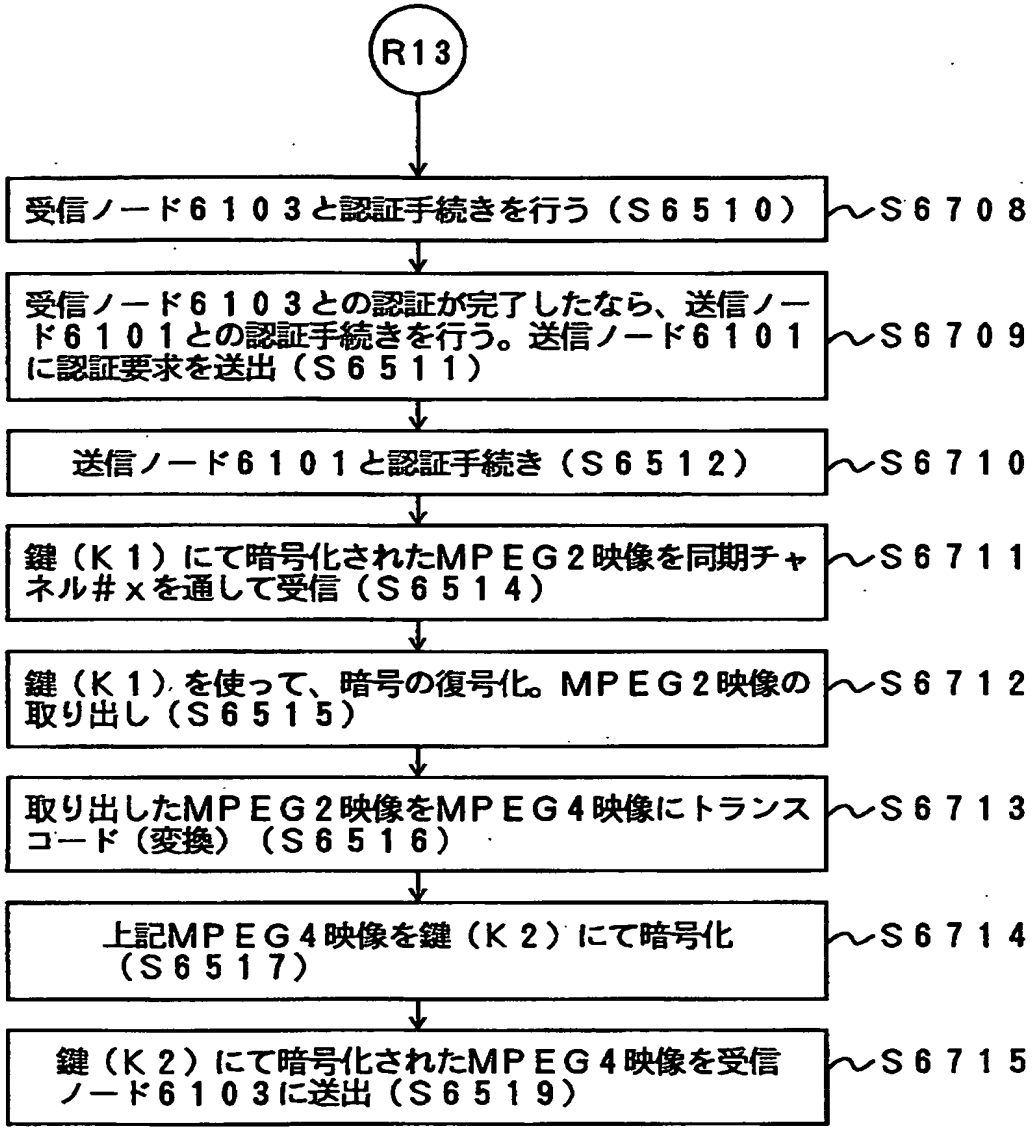
【図６１】


スタート
ホームゲートウエイ６１０２からＩＥＥＥ１２１２レジスタを読まれる（Ｓ６５０１）
～Ｓ６６０１
ホームゲートウエイ６１０２からパネルサブユニットの送信を求められ、送信（Ｓ６５０２）
～Ｓ６６０２
ＡＶ／Ｃプロトコルにて、１３９４バス上に同期チャネル＃ｘを確立し、これを映像送信サブユニットに接続せよ、との命令をホームゲートウエイ６１０２から受信（Ｓ６５０５）
～Ｓ６６０３
同期チャネル＃ｘを介して、暗号化されたＭＰＥＧ２映像を送出（Ｓ６５０７）
～Ｓ６６０４
認証要求を中継ノードから受信（Ｓ６５１１）
～Ｓ６６０５
第１の実施形態と同様の認証・鍵交換手続きを行う（Ｓ６５１２）
～Ｓ６６０６
ＭＰＥＧ２映像を鍵Ｋ１にて暗号化
～Ｓ６６０７
暗号化されたＭＰＥＧ２映像［ＭＰＥＧ２映像］ｋ１を同期チャネル＃ｘを通して送信（Ｓ６５１４）
～Ｓ６６０８

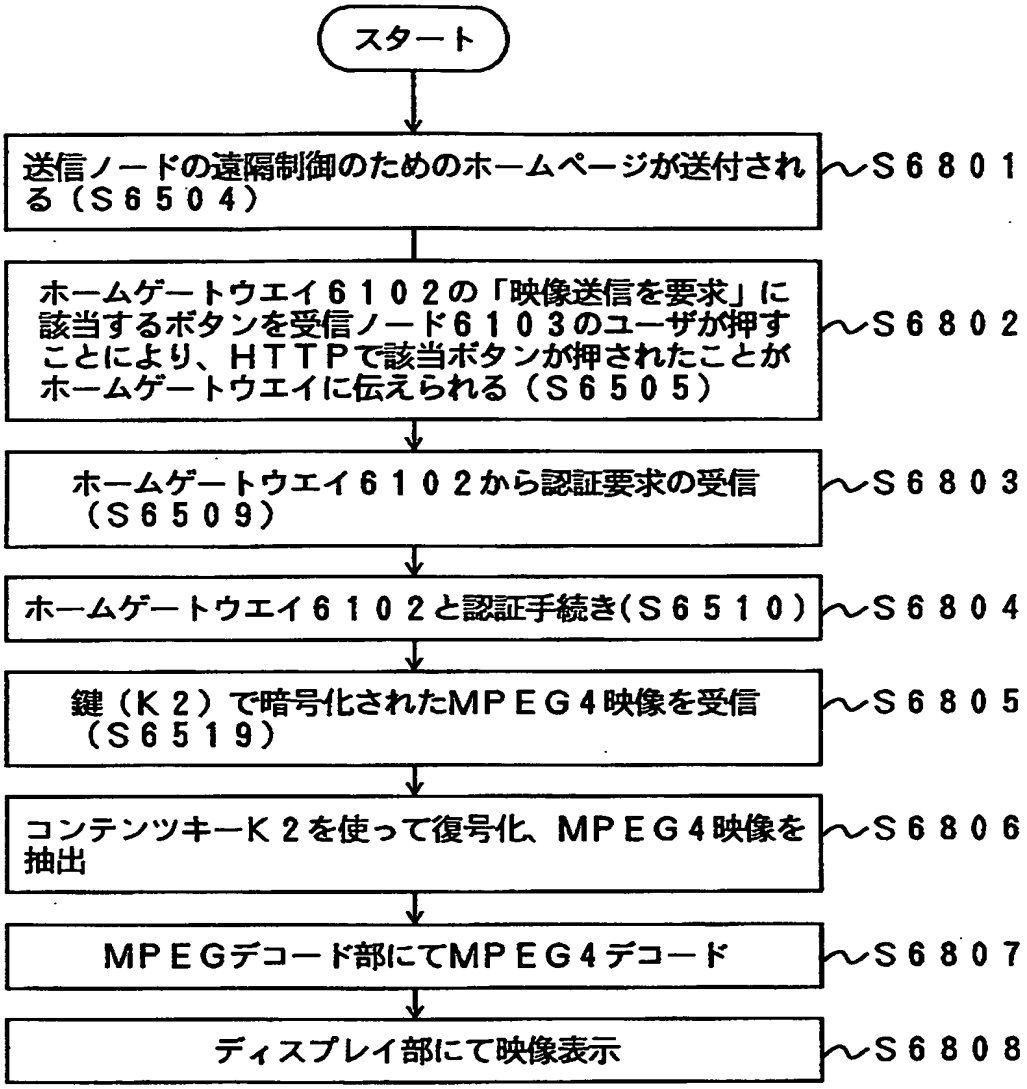
【図６２】


スタート
送信ノード６１０１の構成情報を、送信ノード６１０１のＩＥＥＥ１２１２レジスタを読み込むことにより認識（送信ノードが認証フォーマットを持つことを確認）（Ｓ６５０１）
～Ｓ６７０１
送信ノード６１０１のパネルサブユニットを読み込み（Ｓ６５０２）
～Ｓ６７０２
前記パネル情報をもとに、送信ノード６１０１の遠隔制御用の制御画面をホームページ上に作成。対応関係を変換テーブルに記録。インターネット側に公開（Ｓ６５０３）
～Ｓ６７０３
受信ノード６１０３から、インターネット経由でホームページの操作を受信（例えば再生を意味するボタンが押される）（Ｓ６５０４）
～Ｓ６７０４
変換テーブルを参照し、ＩＥＥＥ１３９４バス上に同期チャネル＃ｘを確保。送信ノード６１０１（の映像送信サブユニット）に対し、同期チャネル＃ｘに対しての映像の送信を要求（Ｓ６５０６）
～Ｓ６７０５
送信ノード６１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ２映像を受信。ＭＰＥＧ２／ＭＰＥＧ４変換ができないことから、これが暗号化されていることを認識（Ｓ６５０７）
～Ｓ６７０６
送信相手（この場合受信ノード６１０３）に対して認証手続きが必要であると認識。受信ノード６１０３に対して認証要求を送出（Ｓ６５０８，Ｓ６５０９）
～Ｓ６７０７
R１３

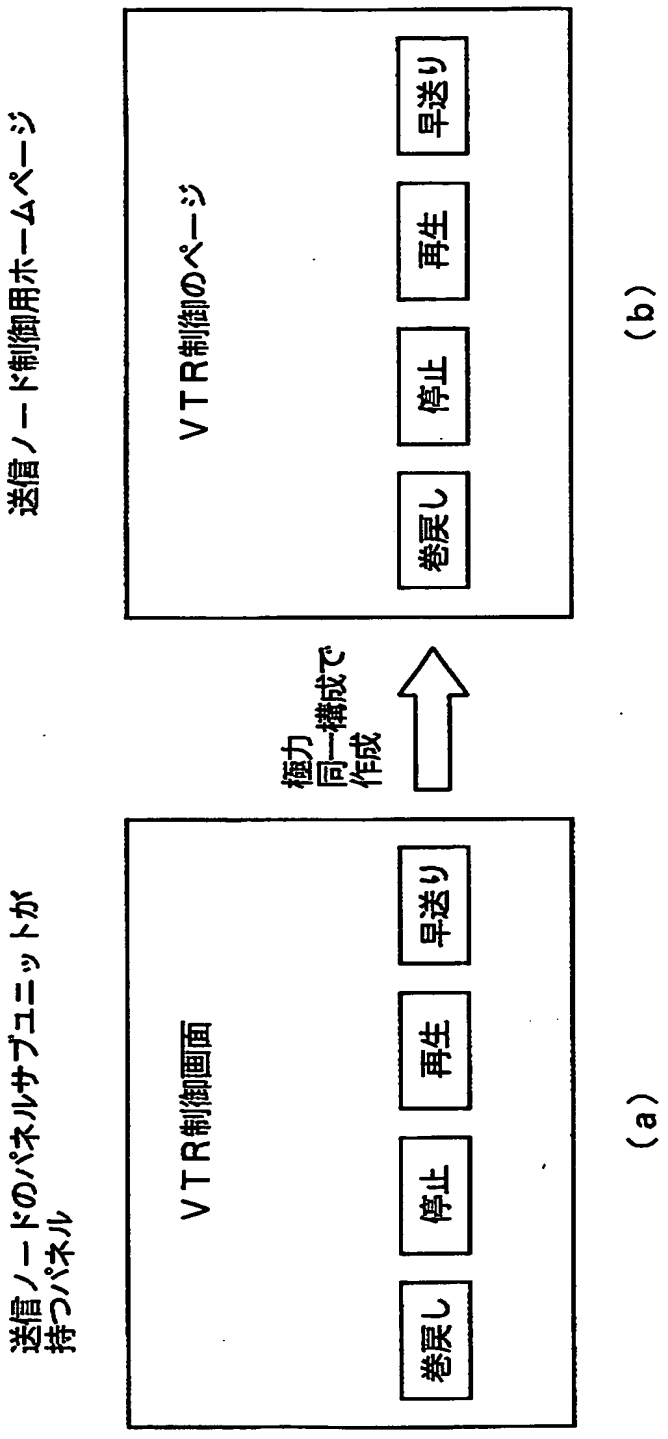
【図６３】


R13
受信ノード６１０３と認証手続きを行う（Ｓ６５１０）
～Ｓ６７０８
受信ノード６１０３との認証が完了したなら、送信ノード６１０１との認証手続きを行う。送信ノード６１０１に認証要求を送出（Ｓ６５１１）
～Ｓ６７０９
送信ノード６１０１と認証手続き（Ｓ６５１２）
～Ｓ６７１０
鍵（Ｋ１）にて暗号化されたＭＰＥＧ２映像を同期チャネル＃ｘを通して受信（Ｓ６５１４）
～Ｓ６７１１
鍵（Ｋ１）を使って、暗号の復号化。ＭＰＥＧ２映像の取り出し（Ｓ６５１５）
～Ｓ６７１２
取り出したＭＰＥＧ２映像をＭＰＥＧ４映像にトランスコード（変換）（Ｓ６５１６）
～Ｓ６７１３
上記ＭＰＥＧ４映像を鍵（Ｋ２）にて暗号化（Ｓ６５１７）
～Ｓ６７１４
鍵（Ｋ２）にて暗号化されたＭＰＥＧ４映像を受信ノード６１０３に送出（Ｓ６５１９）
～Ｓ６７１５

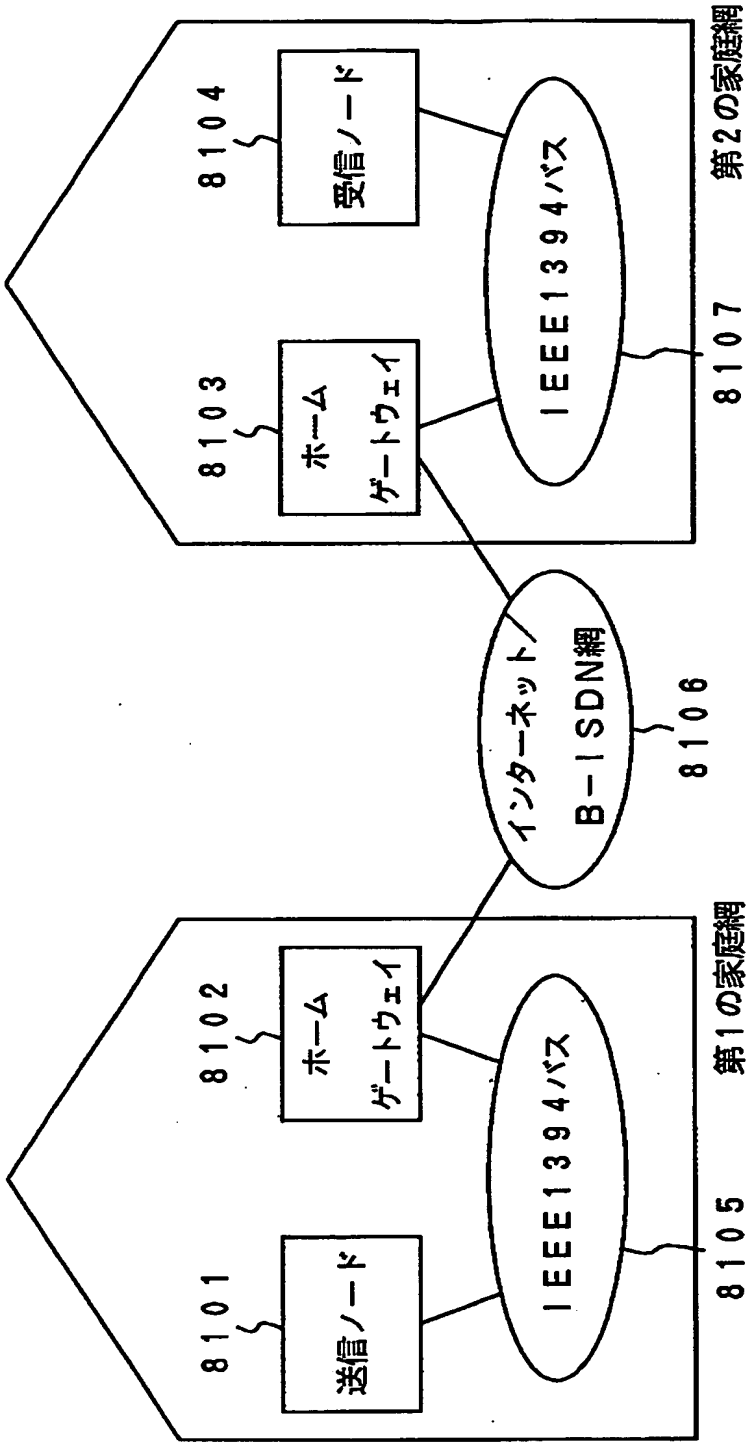
【図６４】


スタート
送信ノードの遠隔制御のためのホームページが送付される（Ｓ６５０４）
～Ｓ６８０１
ホームゲートウエイ６１０２の「映像送信を要求」に該当するボタンを受信ノード６１０３のユーザが押すことにより、ＨＴＴＰで該当ボタンが押されたことがホームゲートウエイに伝えられる（Ｓ６５０５）
～Ｓ６８０２
ホームゲートウエイ６１０２から認証要求の受信（Ｓ６５０９）
～Ｓ６８０３
ホームゲートウエイ６１０２と認証手続き（Ｓ６５１０）
～Ｓ６８０４
鍵（Ｋ２）で暗号化されたＭＰＥＧ４映像を受信（Ｓ６５１９）
～Ｓ６８０５
コンテンツキーＫ２を使って復号化、ＭＰＥＧ４映像を抽出
～Ｓ６８０６
ＭＰＥＧデコード部にてＭＰＥＧ４デコード
～Ｓ６８０７
ディスプレイ部にて映像表示
～Ｓ６８０８

【図６５】

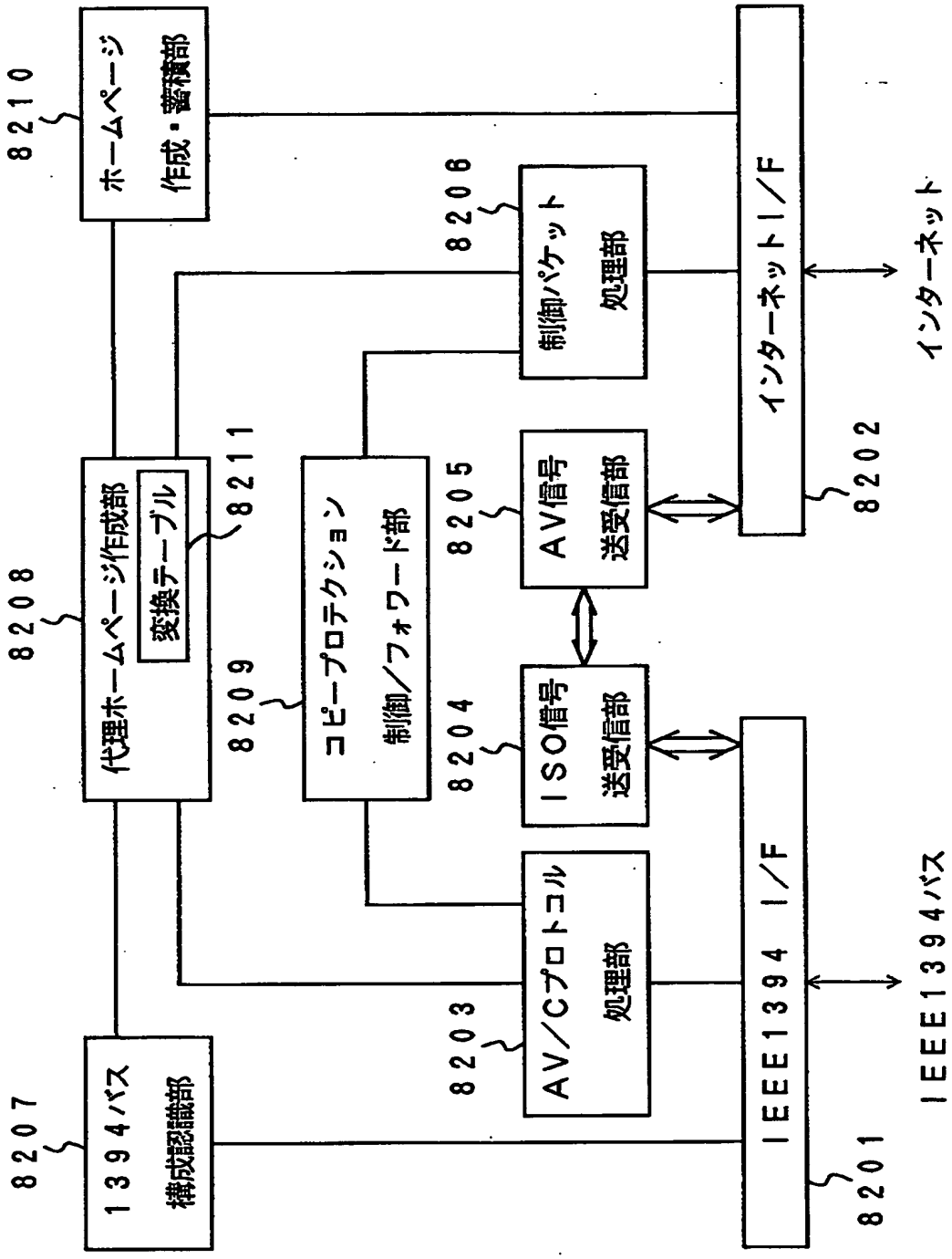

送信ノードのパネルサブユニットが
持つパネル
VTR制御画面
巻戻し
停止
再生
早送り
(a)
極力
同一構成で
作成
送信ノード制御用ホームページ
VTR制御のページ
巻戻し
停止
再生
早送り
(b)

【図６６】

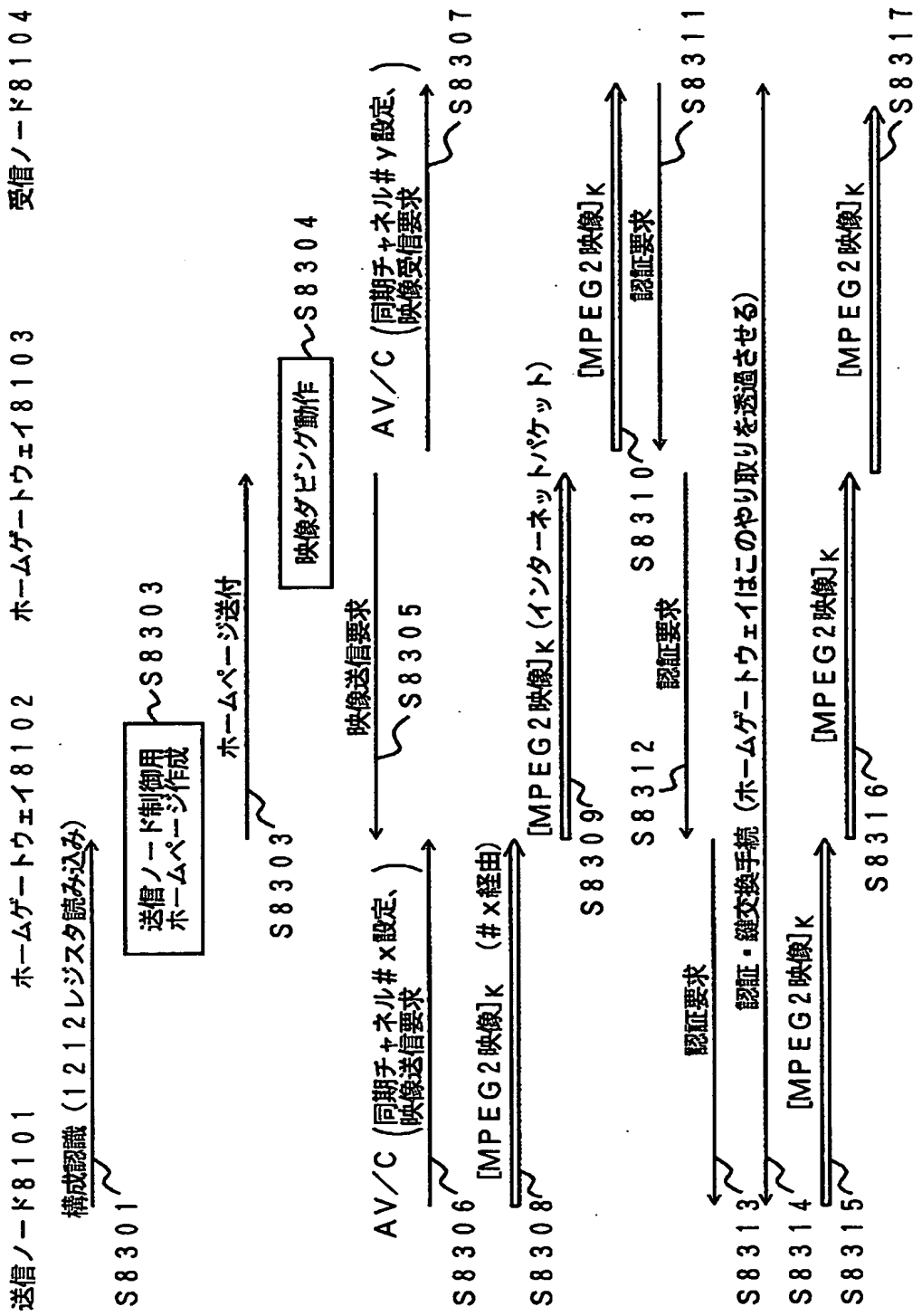


出証特平１１－３０２４２９１

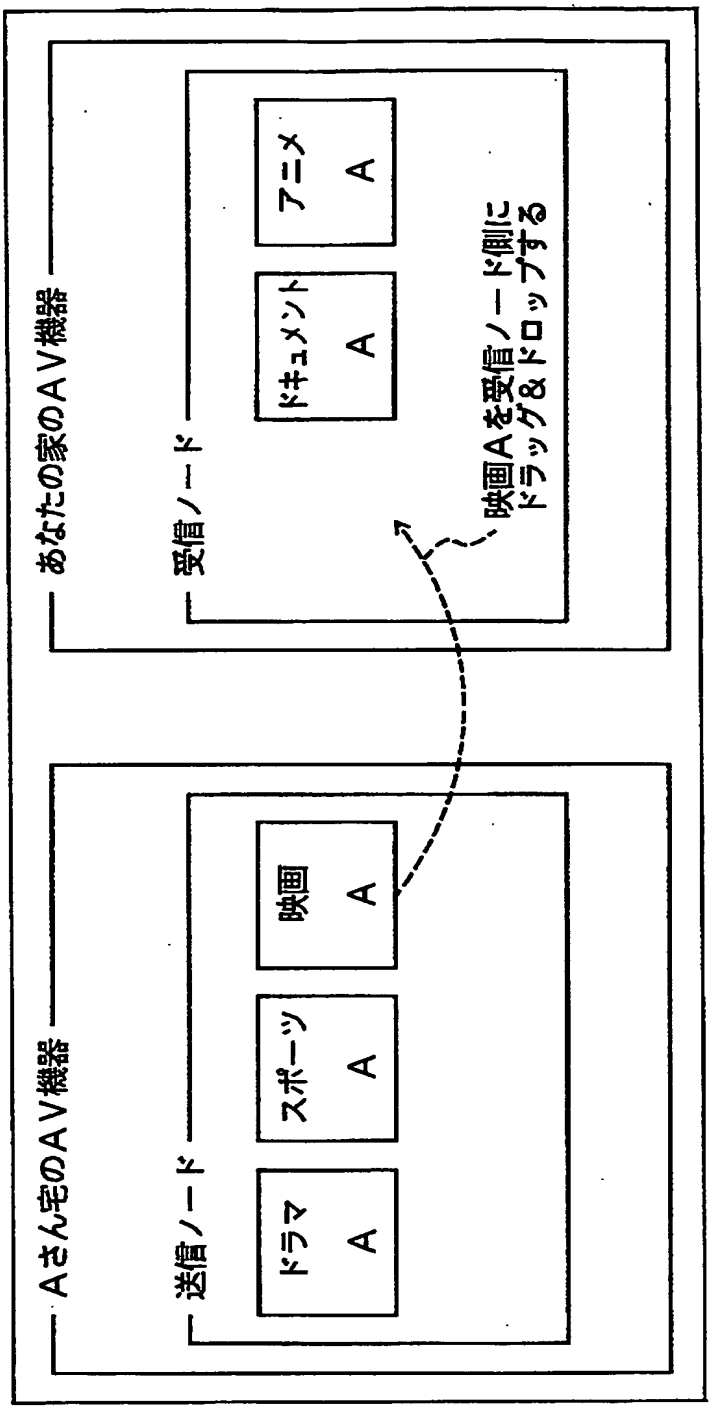
【図６７】


8210
ホームページ
作成・蓄積部
8208
代理ホームページ作成部
変換テーブル
8211
8207
1394バス
構成認識部
8209
コピープロテクション
制御／フォワード部
8206
制御パケット
処理部
8205
AV信号
送受信部
8204
ISO信号
送受信部
8203
AV／Cプロトコル
処理部
8202
インターネットI／F
インターネット
8201
IEEE1394 I／F
IEEE1394バス

【図６８】


送信ノード8101
ホームゲートウェイ8102
ホームゲートウェイ8103
受信ノード8104
構成認識（1212レジスタ読み込み）
S8301
送信ノード制御用ホームページ作成
S8303
ホームページ送付
S8303
映像ダビング動作
S8304
AV／C（同期チャネル#y設定、映像受信要求）
S8307
映像送信要求
S8305
AV／C（同期チャネル#x設定、映像送信要求）
S8306
[MPEG2映像]K（#x経由）
S8308
[MPEG2映像]K（インターネットパケット）
S8309
[MPEG2映像]K
S8310
認証要求
S8312
認証要求
S8311
認証要求
S8313
認証・鍵交換手続（ホームゲートウェイはこのやり取りを透過させる）
S8314
[MPEG2映像]K
S8315
[MPEG2映像]K
S8316
[MPEG2映像]K
S8317

【図６９】


Aさん宅のAV機器
送信ノード
ドラマ A
スポーツ A
映画 A
あなたの家のAV機器
受信ノード
ドキュメント A
アニメ A
映画Aを受信ノード側に
ドラッグ&ドロップする

【書類名】　　要約書

【要約】

【課題】　同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。

【解決手段】　第１のネットワークに接続されたインタフェースと、第２のネットワークに接続されたインタフェースと、第２のネットワーク上の装置又はサービス又はサブユニットを自中継装置上のものとして第１のネットワーク側に開示し、この装置又はサービス又はサブユニット宛の第１の情報を代理で受信し、該第２のネットワーク上の装置又はサービス又はサブユニットへの第２の情報に変換して送信する代理構成機能と、第１のネットワーク上の装置からの第１の情報を受信した際この情報が少なくとも所定の情報であるか否かを検出する機能と、検出した第１の情報が所定の情報であった場合にはこの所定の情報を第２のネットワーク上の装置又はサービス又はサブユニットに転送する機能とを有する。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000003078
【住所又は居所】　神奈川県川崎市幸区堀川町７２番地
【氏名又は名称】　株式会社東芝
【代理人】　申請人
【識別番号】　100058479
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　鈴江　武彦
【選任した代理人】
【識別番号】　100084618
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　橋本　良郎
【選任した代理人】
【識別番号】　100091351
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河野　哲
【選任した代理人】
【識別番号】　100088683
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　中村　誠
【選任した代理人】

【識別番号】　100070437
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河井　将次

出 願 人 履 歴 情 報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝